Investigación sobre caso “Cebolla Chan” - versión 1.0



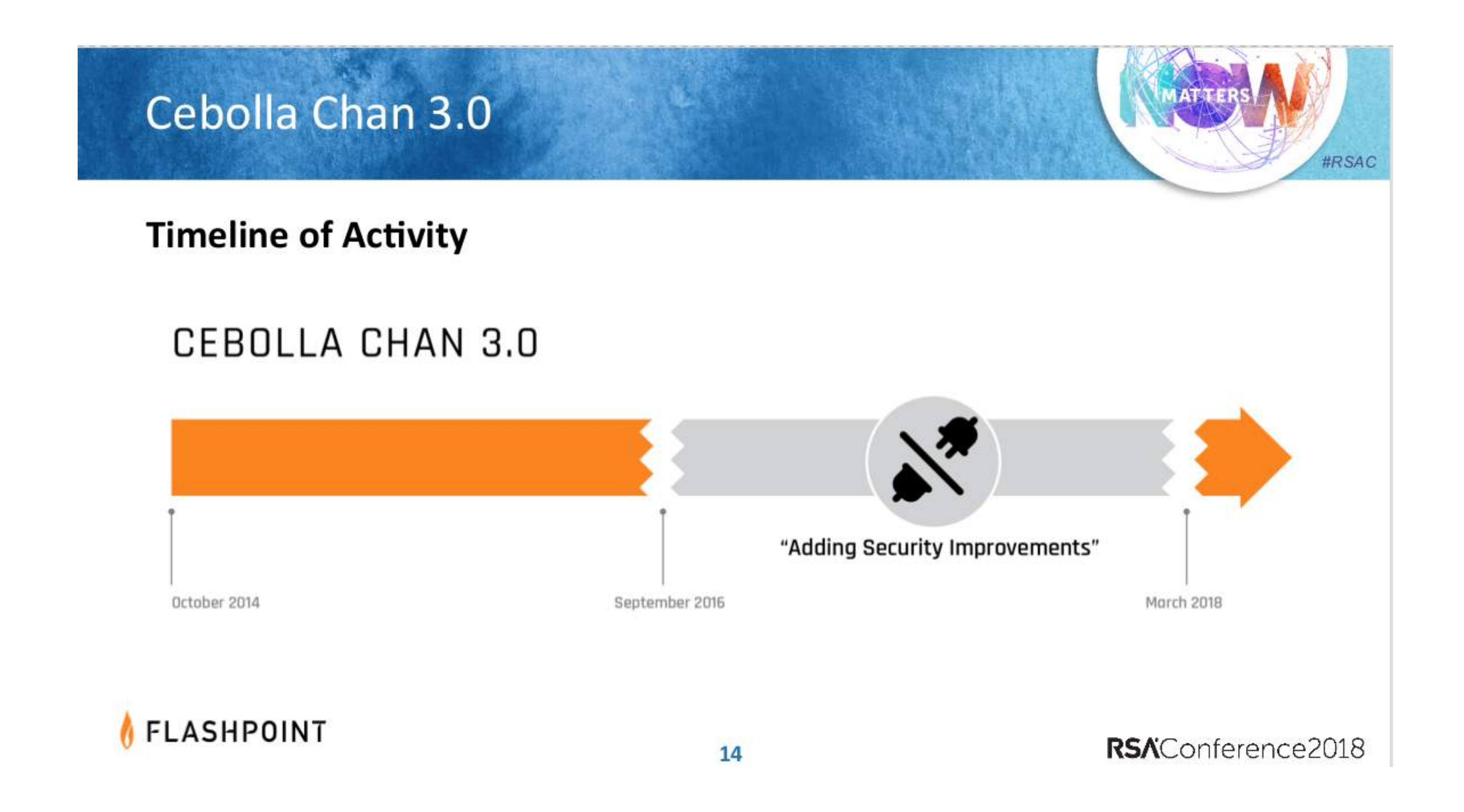
(Edit: al momento de retomar este documento han pasado meses desde que comencé a redactarlo, algunos sitios están offline pero trataré de reestructurar todo a lo largo del mismo).

Este documento recopila información valiosa que he analizado por algunos meses, fruto de análisis lógico y aplicación de técnicas básicas de osint.

A continuación mediante el presente e-book les muestro parte de mi investigación que busca generar un análisis sobre la estructura de cierto núcleo de actividad hispana en la darkweb

Cebolla Chan es una comunidad underground que data desde el 17 de octubre de 2014, que actualmente tiene alrededor de 108,000 miembros registrados y 108,667 mensajes en 19,823 temas según las estadísticas del foro a la fecha, es un foro generalista con temáticas entre ellas están: Inteligencia, Erótica, Ingeniería financiera, Bolsa de empleo.

El foro cerró temporalmente por cuestiones de seguridad según el admin SysOp allá por septiembre del 2016 como podemos notar en el siguiente gráfico que tomé de:
https://www.rsaconference.com/industry-topics/presentation/cebolla-chan-30-a-window-into-the-chaotic-spanishlanguage-underground
&&
https://www.flashpoint-intel.com/blog/podcasts/collective-intelligence-podcast-spanish-language-cybercrime-underground/



Y un día allá por el 12 de abril de 2018 todo volvió a funcionar:

Bienvenid@s a Cebolla Chan 3.0 // 2018 // - Tor Browser

Bienvenid@s a Cebolla Chan 3.0 | Navegación privada

s6cco2jylmxqcdeh.onion/w/showthread.php?tid=26793

¡Hola, Invitado! Iniciar sesión Regístrate | Buscar (by TORCH)

Cebolla Chan 3.0 › Cebolla Chan › Cebolla Chan Info

Bienvenid@s a Cebolla Chan 3.0 // 2018 //

TOR SCAM LIST

Páginas (7): 1 2 3 4 5 ... 7 Siguiente » | Calificación:

Bienvenid@s a Cebolla Chan 3.0 // 2018 // | Modos de tema

2018-03-12, 10:20 PM #1

SysOp
Administrator
Mensajes: 297
Temas: 38
Registro en: Oct 2014
Reputación: 29

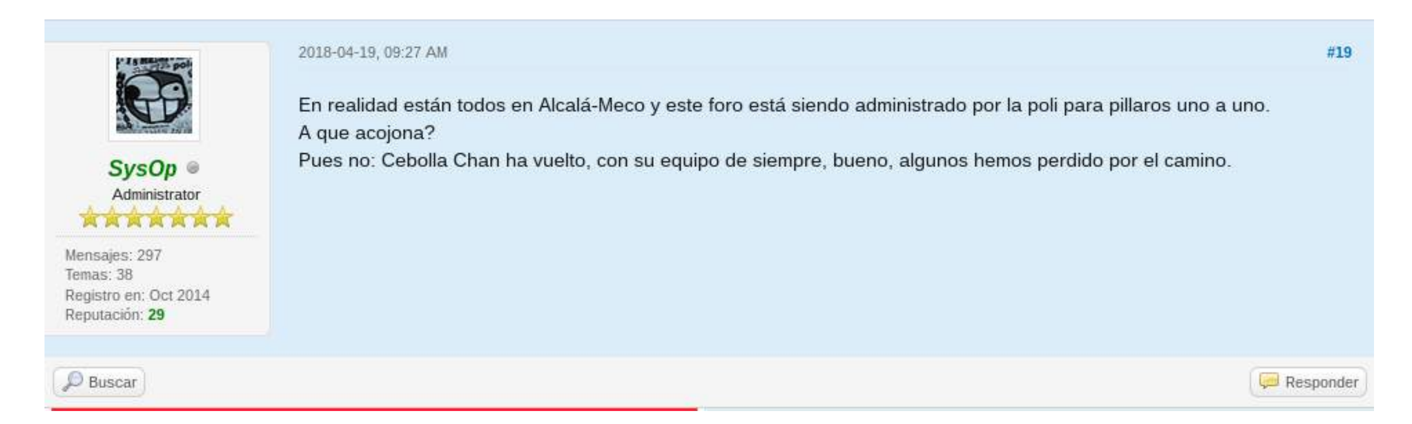
Cebolla Chan, el auténtico, el legendario, ha vuelto.

Se conservaron los usuarios, hilos, posts, privados, etc, que había en 2016 antes de cerrar el foro.
Las normas serán revisadas para adaptarlas a la actualidad.

SysOp

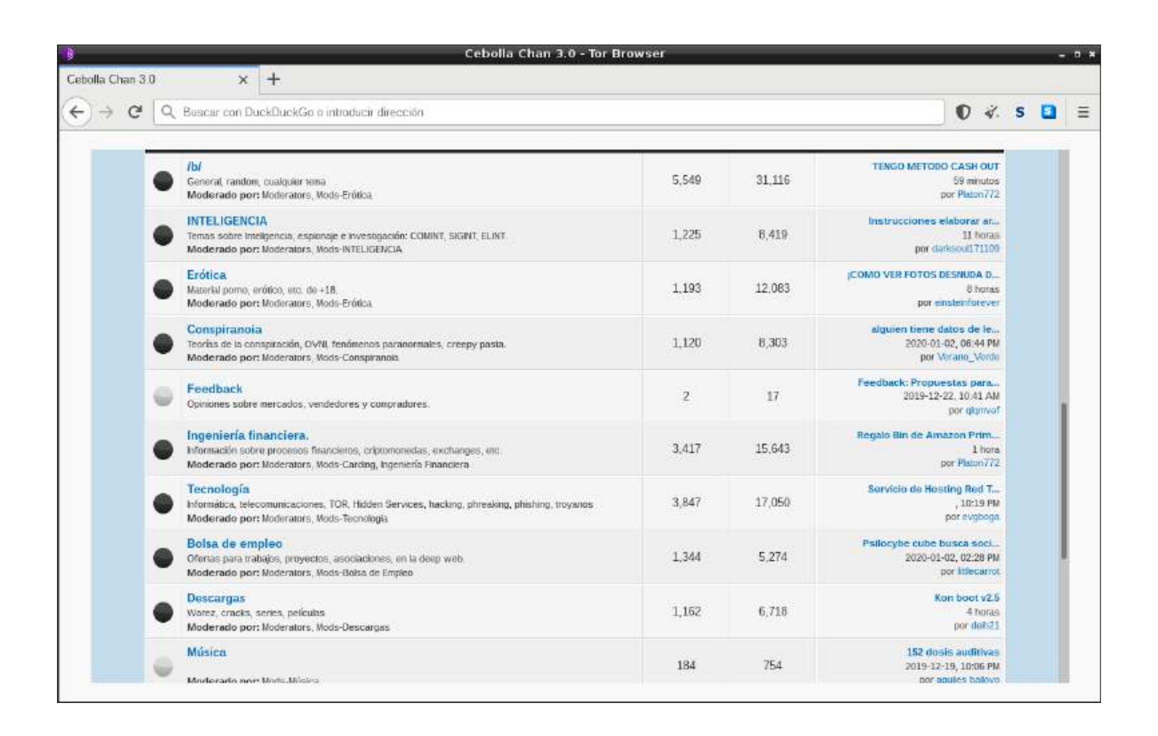
Buscar | Responder

2018-03-12, 11:50 PM #2

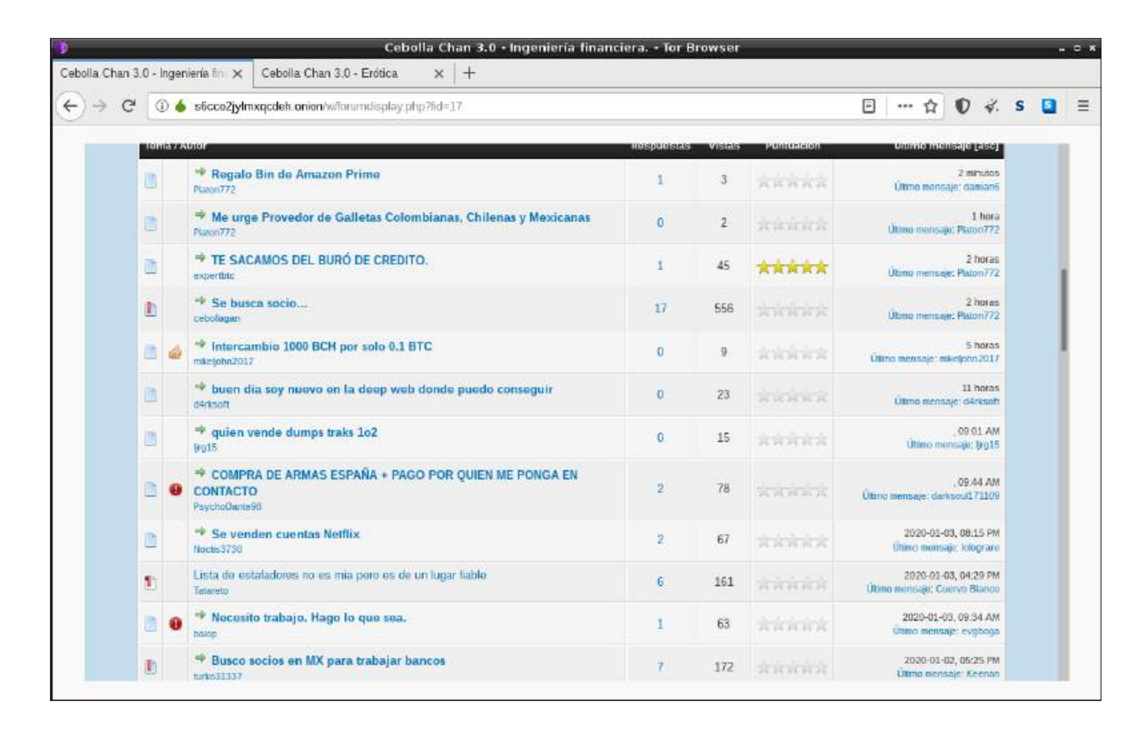


Claro, antes se envió un email a todos los usuarios invitándoles a regresar al foro:

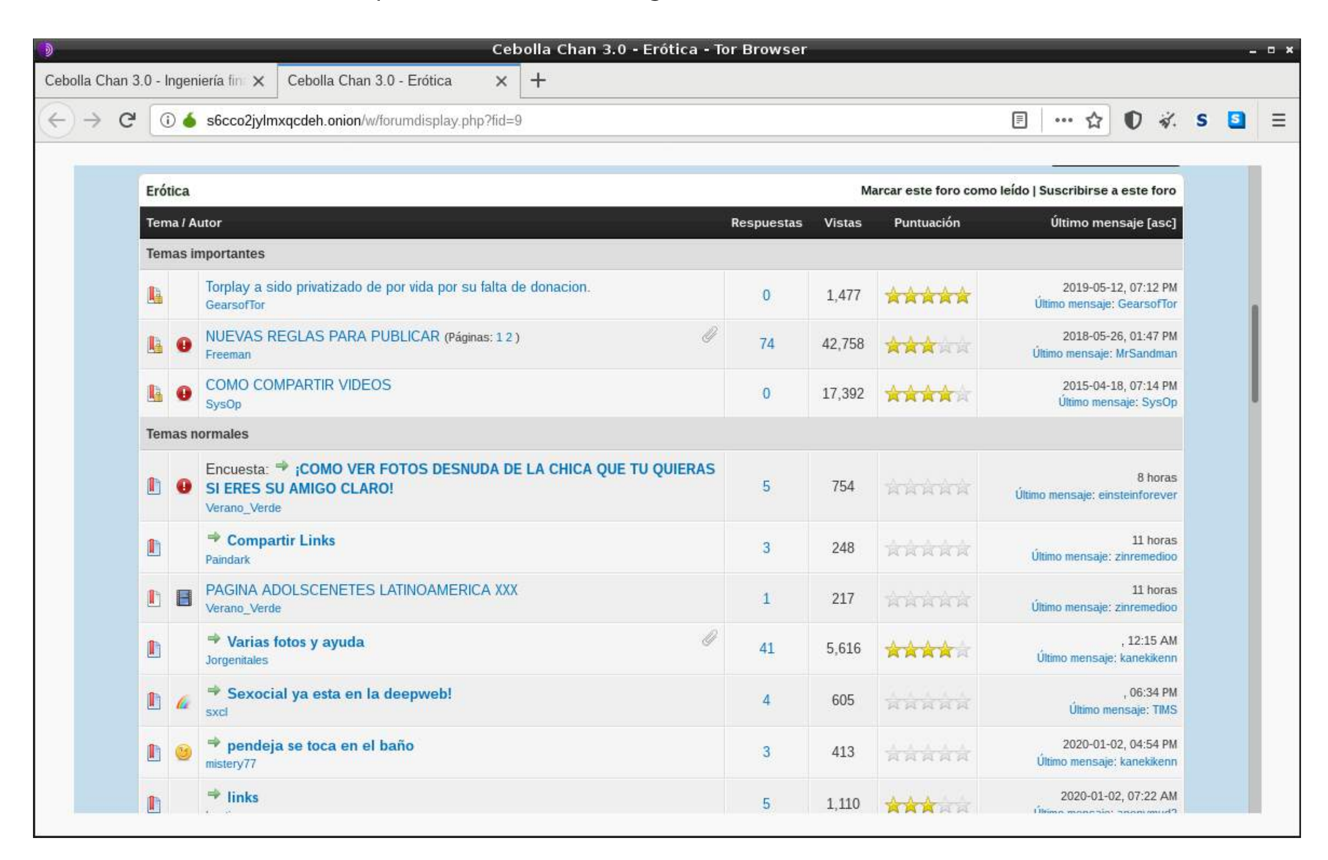
> soy SysOp, de Cebolla Chan 3.0 y te escribo para anunciarte que el foro vuelve a estar en línea y por mucho tiempo.
>
> Como sabes, Cebolla Chan 3.0 cerró de forma preventiva dado que la infraestructura de sistemas donde se alojaba no era lo suficientemente segura. Durante este tiempo he estado montando una estructura desde cero para que el foro pueda ser operado con seguridad y fiabilidad.
>
> Te animo a que vuelvas: está todo igual que el último día en 2016. Encontrarás todos los hilos y más de cien mil mensajes.
>
> Bienvenid@ de nuevo
>
> SysOp
>
> http://s6cco2jylmxqcdeh.onion



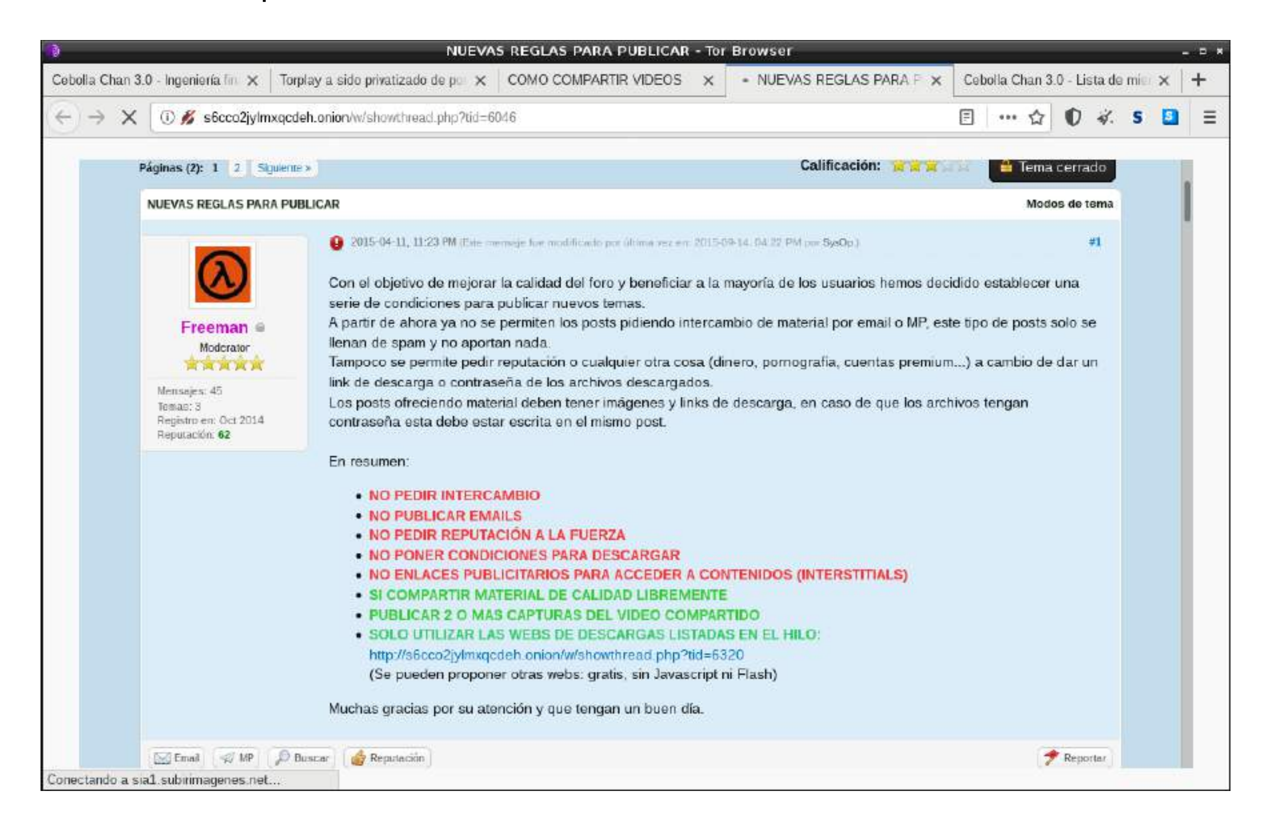
En el foro podemos notar que entre los las secciones con mayor actividad está /b/ que son publicaciones sin una temática definida, Erótica que es una sección llena de jailbait, porno de venganza, e intercambio de pornografía infantil; valga la redundancia y Ingeniería financiera/Bolsa de empleo/Feedback que están orientadas a cibercriminales que intercambian/compran/venden contactos, información bancaria, además de reclutar personas para hacer sus fechorías.



Captura de foro "Ingeniería financiera".



Detalle interesante:
Ahora nos vamos con el foro erótica, y aquí tenemos las reglas del mismo escritas por el moderador "Freeman" el 11 de abril de 2015:



Transcripción:

Con el objetivo de mejorar la calidad del foro y beneficiar a la mayoría de los usuarios hemos decidido establecer una serie de condiciones para publicar nuevos temas.
A partir de ahora ya no se permiten los posts pidiendo intercambio de material por email o MP, este tipo de posts solo se llenan de spam y no aportan nada.

Tampoco se permite pedir reputación o cualquier otra cosa (dinero, pornografía, cuentas premium...) a cambio de dar un link de descarga o contraseña de los archivos descargados.
Los posts ofreciendo material deben tener imágenes y links de descarga, en caso de que los archivos tengan contraseña esta debe estar escrita en el mismo post.

En resumen:

- **NO PEDIR INTERCAMBIO**
- **NO PUBLICAR EMAILS**
- **NO PEDIR REPUTACIÓN A LA FUERZA**
- **NO PONER CONDICIONES PARA DESCARGAR**
- **NO ENLACES PUBLICITARIOS PARA ACCEDER A CONTENIDOS (INTERSTITIALS)**
- **SI COMPARTIR MATERIAL DE CALIDAD LIBREMENTE**
- **PUBLICAR 2 O MAS CAPTURAS DEL VIDEO COMPARTIDO**
- **SOLO UTILIZAR LAS WEBS DE DESCARGAS LISTADAS EN EL HILO:** http://s6cco2jylmxqcdeh.onion/w/showthread.php?tid=6320
  (Se pueden proponer otras webs: gratis, sin Javascript ni Flash)

Muchas gracias por su atención y que tengan un buen día.

Al link que redirige es a uno del administrador del foro llamdo "Sysop" que transcribiré a continuación:

2015-04-18, 07:14 PM (Este mensaje fue modificado por última vez en: 2018-04-12, 02:35 PM por SysOp.)
Es importante subir los videos a webs de descargas que permitan trabajar sin Javascript y es preferible que se encuentren en Tor.

Como últimamente en Tor nos estamos quedando sin servicios de descarga de ficheros, podemos utilizar la siguiente web:

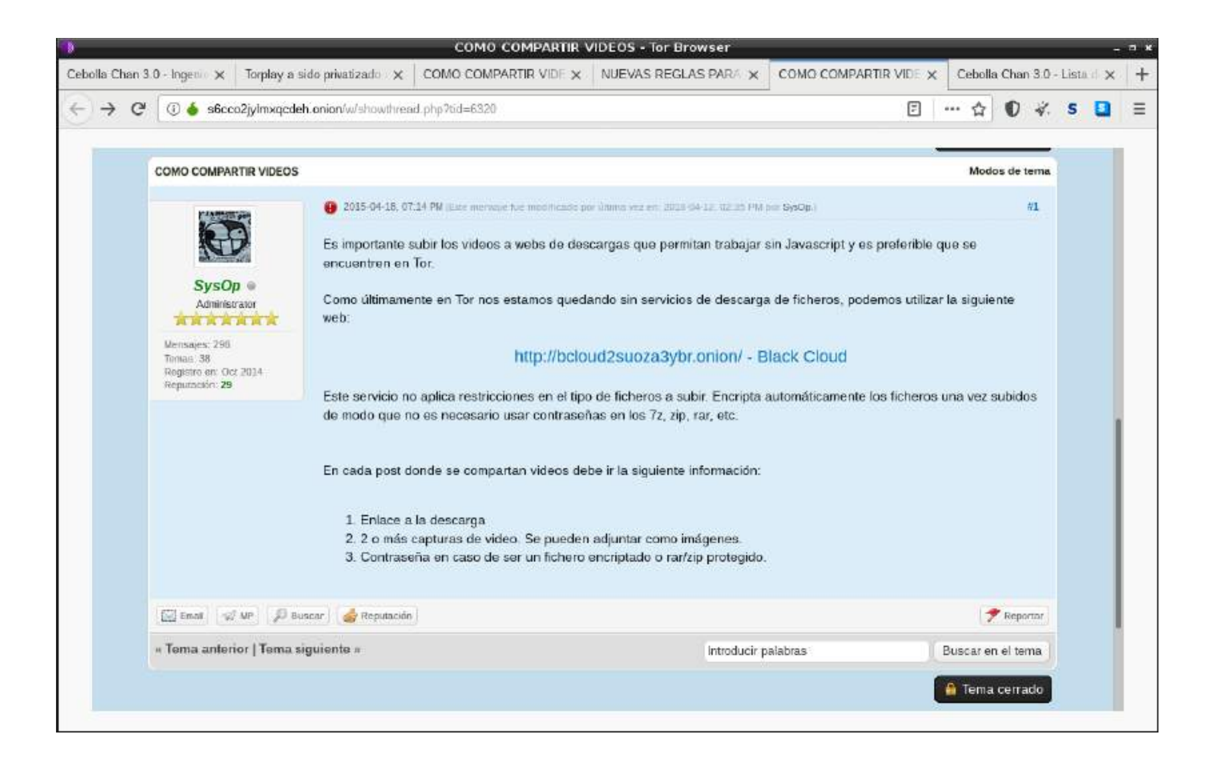
http://bcloud2suoza3ybr.onion/ - Black Cloud

Este servicio no aplica restricciones en el tipo de ficheros a subir. Encripta automáticamente los ficheros una vez subidos de modo que no es necesario usar contraseñas en los 7z, zip, rar, etc.

En cada post donde se compartan videos debe ir la siguiente información:

1. Enlace a la descarga

2. 2 o más capturas de video. Se pueden adjuntar como imágenes.
3. Contraseña en caso de ser un fichero encriptado o rar/zip protegido.

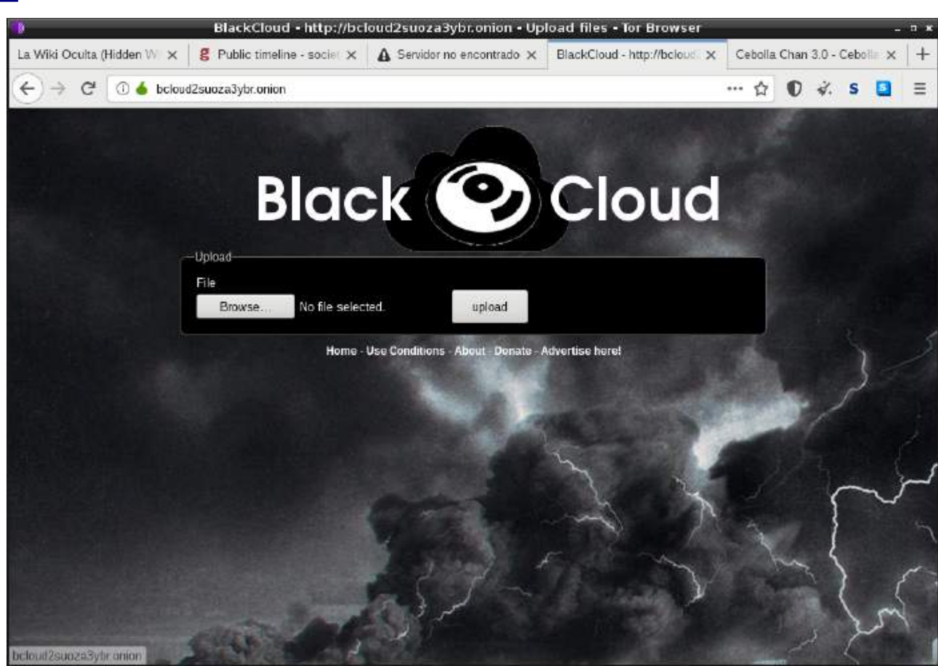


Bueno tomando en cuenta que bcloud es un servicio que ha sido publicitado principalmente por cebolla chan podemos hacer nuestras propias especulaciones acerca de ello…

http://bcloud2suoza3ybr.onion/

http://archive.is/ZCQ6P

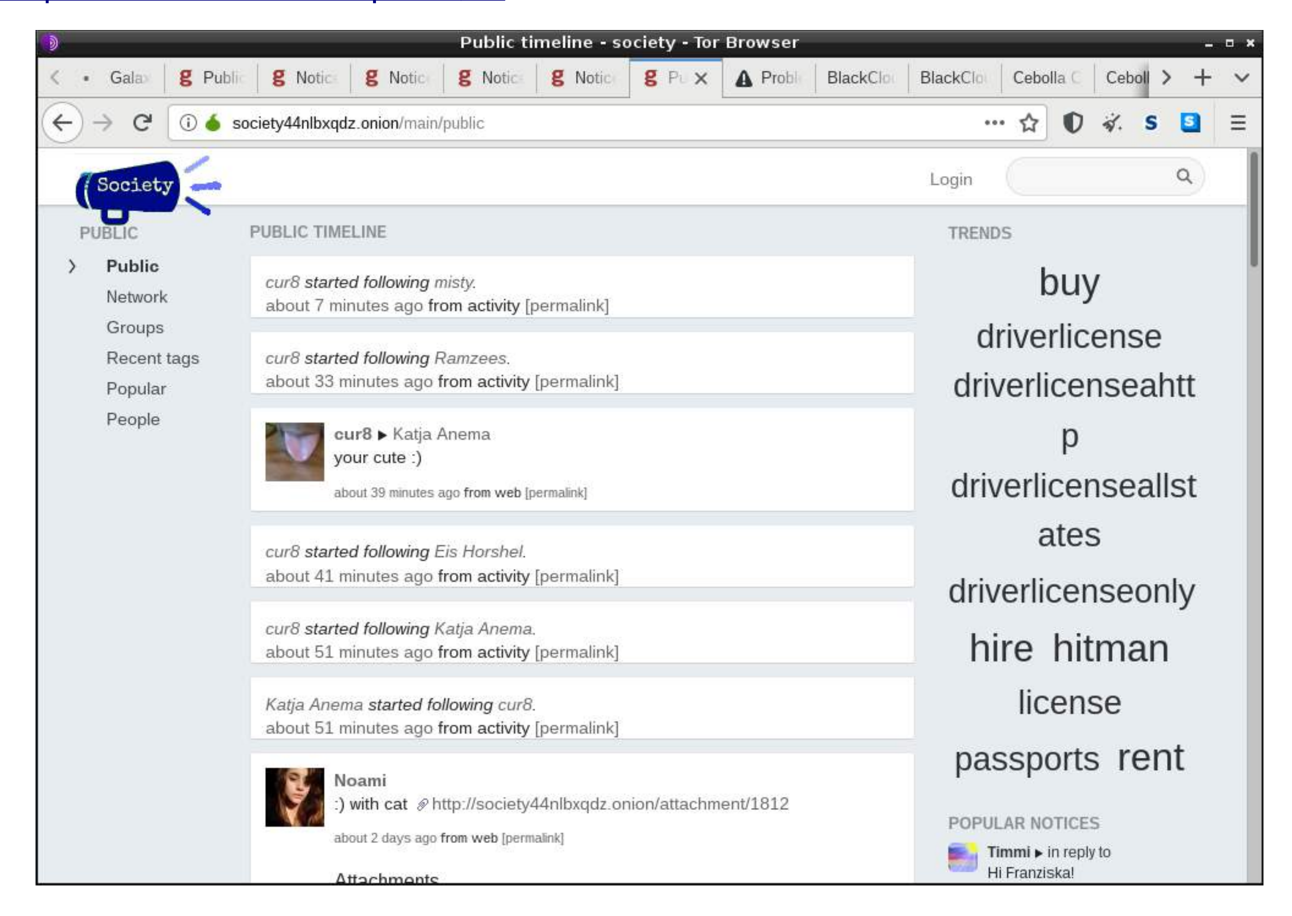
Black Cloud, servicio de intercambio de archivos anónimo que permite la subida de cualquier tipo de archivo/contenido.



Ahora vamos con otro sitio que es promocionado por el foro, una red social de microblogging basada en Gnusocial que fué puesta en línea el 7 de febrero de 2018.

http://society44nlbxqdz.onion

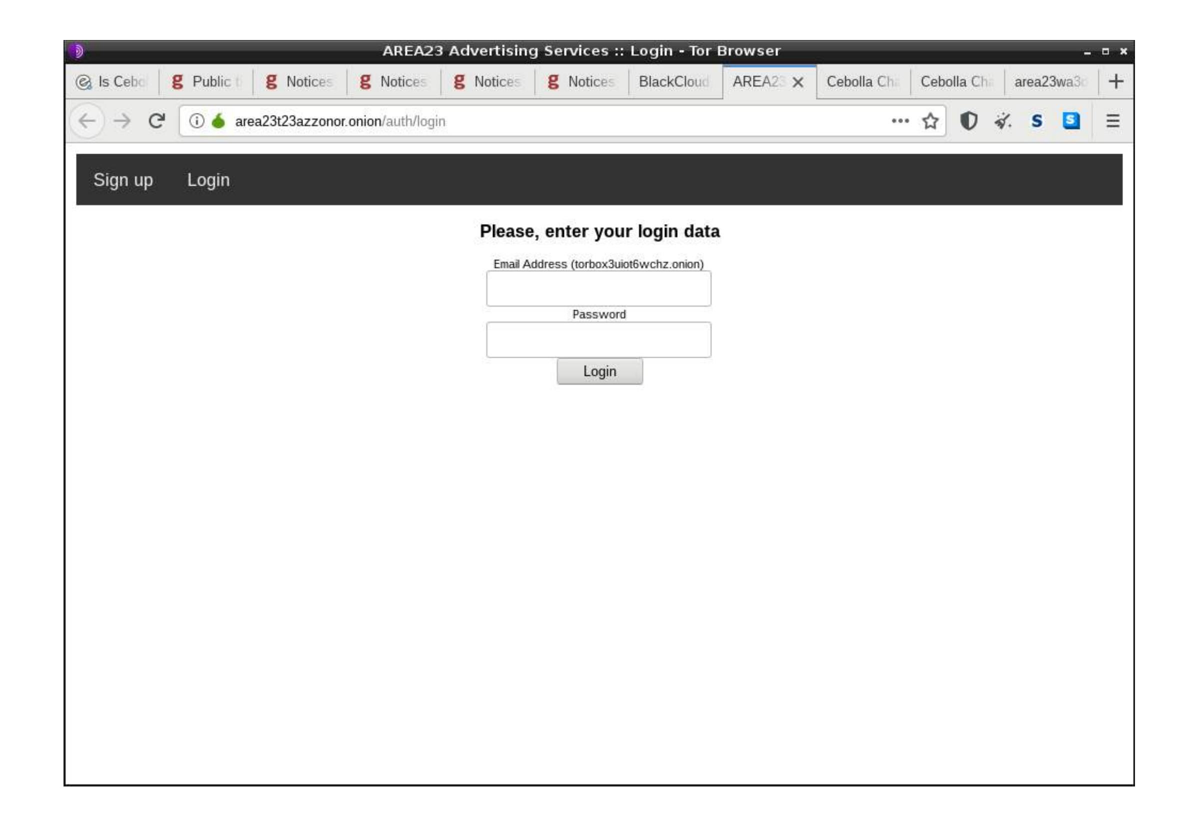
http://archive.is/wip/v9QxM



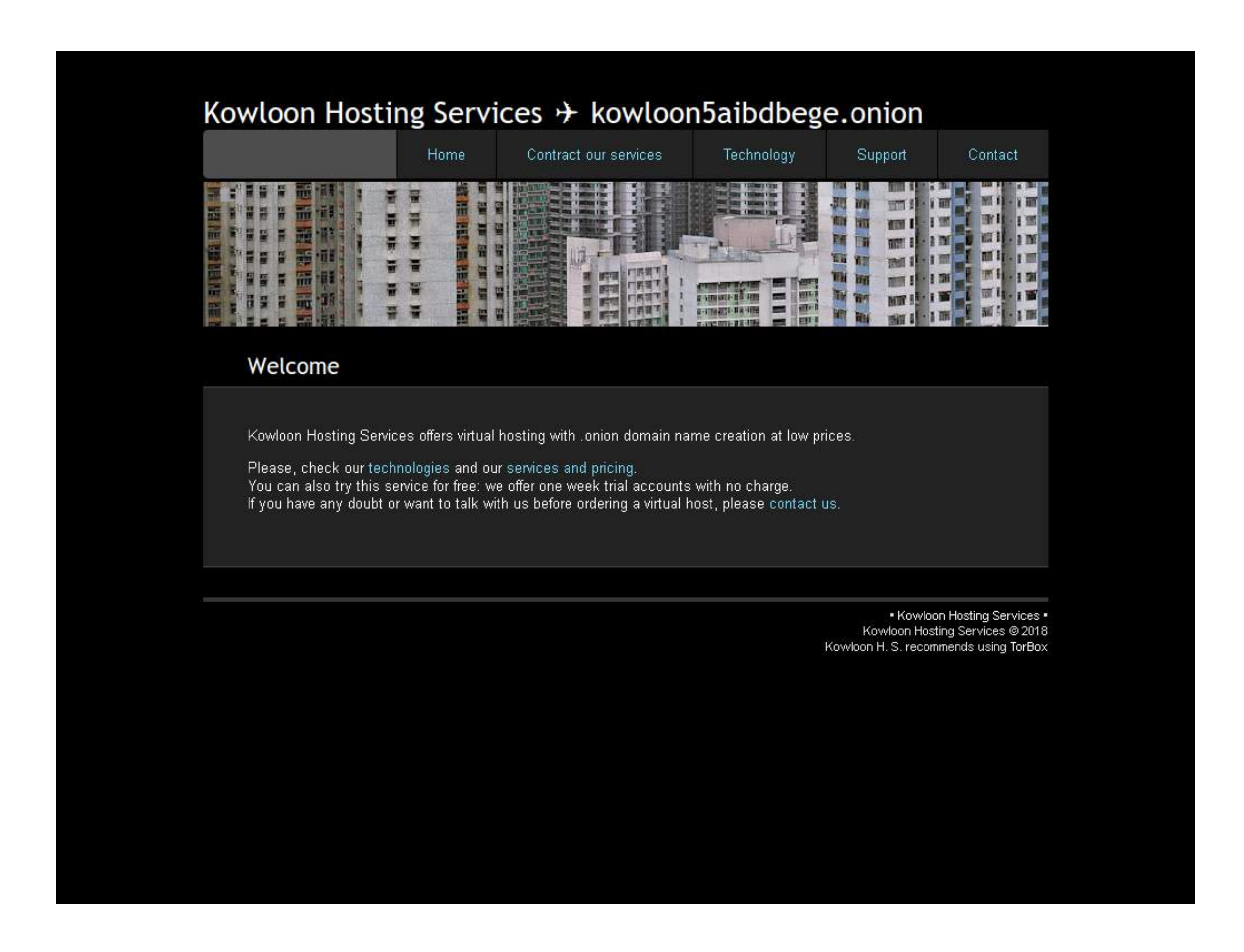
Luego seguimos con un sitio de publicidad al que hacen referencia cebolla chan y blackcloud, “area32”, campañas de publicidad en la red tor, algo emprendedor no?

area23wa3d32yygu.onion

http://archive.is/OkoUL



A continuación tenemos el sitio de hosting en la darkweb “kowloon hosting” que ofrece alojamiento en la darknet de forma fácil y práctica.



http://kowloon5aibdbege.onion/

http://archive.is/Q2AAl

Además de un sitio que se dedica a subir fotos eróticas de dudosa legalidad “The beauty”, no subiré el screenshot por cuestiones legales.

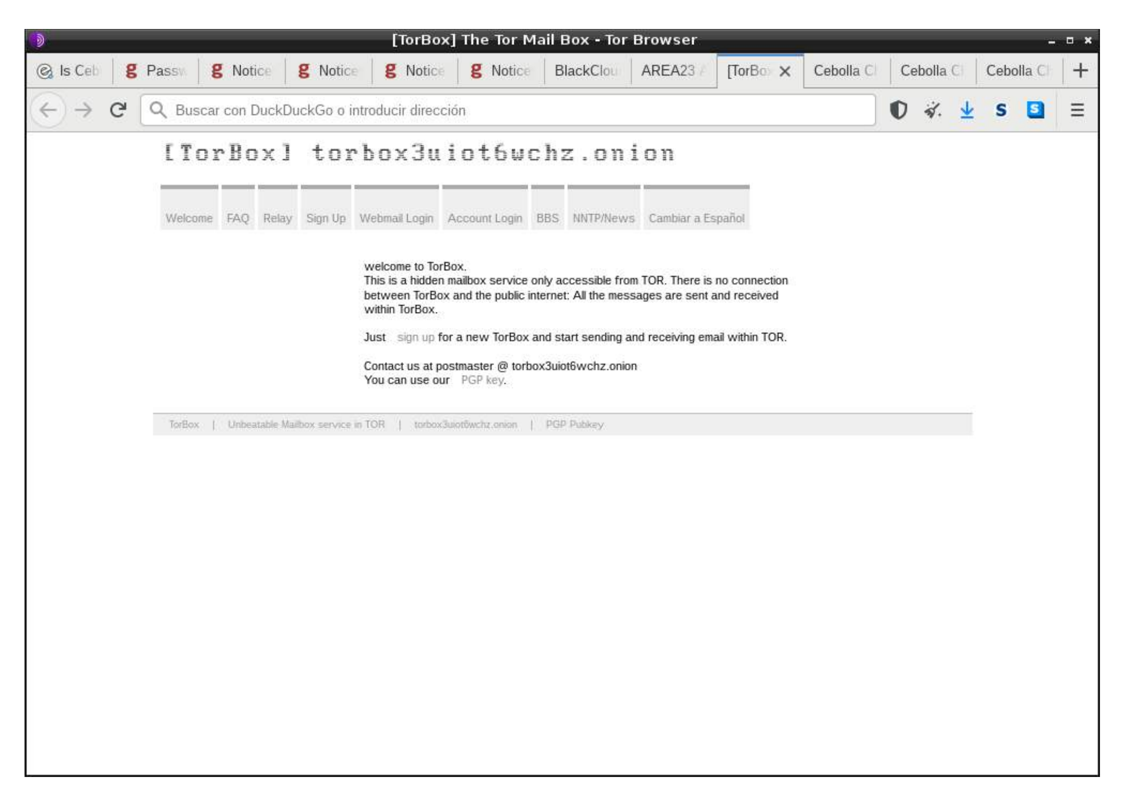
lulzwrzcle5ks3se.onion

http://archive.is/F4iVi

Y para finalizar tenemos al famoso sitio de email gratuito en tor "Torbox", noten que todos los sitios que he mencionado anteriormente recomiendan mucho a este servicio, algo muy interesante.

torbox3uiot6wchz.onion

http://archive.is/csnrl



Pondré los headers de cada sitio por aquí:

area23wa3d32yygu.onion

HTTP/1.1 200 OK

Server: nginx

Date: Mon, 16 Mar 2020 03:19:56 GMT

Content-Type: text/html

Content-Length: 0

Last-Modified: Thu, 26 Jul 2018 22:05:05 GMT

ETag: "5b5a4591-0"

Accept-Ranges: bytes

http://s6cco2jylmxqcdeh.onion

HTTP/1.1 200 OK

Date: Mon, 16 Mar 2020 03:01:45 GMT

Server: Apache

Last-Modified: Mon, 12 Mar 2018 21:14:43 GMT

ETag: "1b3190-271-5673da177fee3"

Accept-Ranges: bytes

Content-Length: 625

Content-Type: text/html

"x-powered-by": "PHP/5.6.32"

torbox3uiot6wchz.onion

HTTP/1.1 200 OK

Date: Mon, 16 Mar 2020 03:22:14 GMT

Server: Apache/2.4.10 (Debian)

Content-Type: text/html; charset=UTF-8

http://society44nlbxqdz.onion

HTTP/1.1 303 See Other

Date: Mon, 16 Mar 2020 03:20:41 GMT

Server: Apache/2.4.10 (Debian) SVN/1.8.10 mod_fcgid/2.3.9 mpm-itk/2.4.7-02 PHP/5.6.40-0+deb8u8 OpenSSL/1.0.1t

X-Powered-By: PHP/5.6.40-0+deb8u8

Vary: Accept-Encoding,Cookie

Location: http://society44nlbxqdz.onion/main/all

Content-Type: text/html; charset=UTF-8

http://bcloud2suoza3ybr.onion/

HTTP/1.1 200 OK

Date: Mon, 16 Mar 2020 03:35:24 GMT

Server: Apache/2.4.10 (Debian) SVN/1.8.10 mod_fcgid/2.3.9 mpm-itk/2.4.7-02 PHP/5.6.40-0+deb8u8 OpenSSL/1.0.1t

X-Powered-By: PHP/5.6.40-0+deb8u8

Content-Type: text/html; charset=UTF-8

http://kowloon5aibdbege.onion/

HTTP/1.1 200 OK

Date: Mon, 16 Mar 2020 03:35:20 GMT

Server: Apache/2.4.10 (Debian) SVN/1.8.10 mod_fcgid/2.3.9 mpm-itk/2.4.7-02 PHP/5.6.40-0+deb8u8 OpenSSL/1.0.1t

Last-Modified: Sat, 09 Mar 2019 09:37:13 GMT

ETag: "722-583a6158e2440"

Accept-Ranges: bytes

Content-Length: 1826

Vary: Accept-Encoding

Content-Type: text/html

lulzwrzcle5ks3se.onion

HTTP/1.1 303 See Other

Date: Wed, 18 Mar 2020 01:44:13 GMT

Server: Apache/2.4.10 (Debian) SVN/1.8.10 mod_fcgid/2.3.9 mpm-itk/2.4.7-02 PHP/5.6.40-0+deb8u8 OpenSSL/1.0.1t

X-Powered-By: PHP/5.6.40-0+deb8u8

Location: http://lulzwrzcle5ks3se.onion/g2/

Content-Type: text/html; charset=UTF-8

De estos sitios vamos a empezar, actualmente todos ellos están en línea y desde ellos vamos a realizar correlaciones que nos permitirán ir descubriendo poco a poco el iceberg.

Para empezar quiero destacar que los siguientes sitios tienen la misma huella digital cuando revisamos las cabeceras con el comando “torsocks curl -I link.onion”

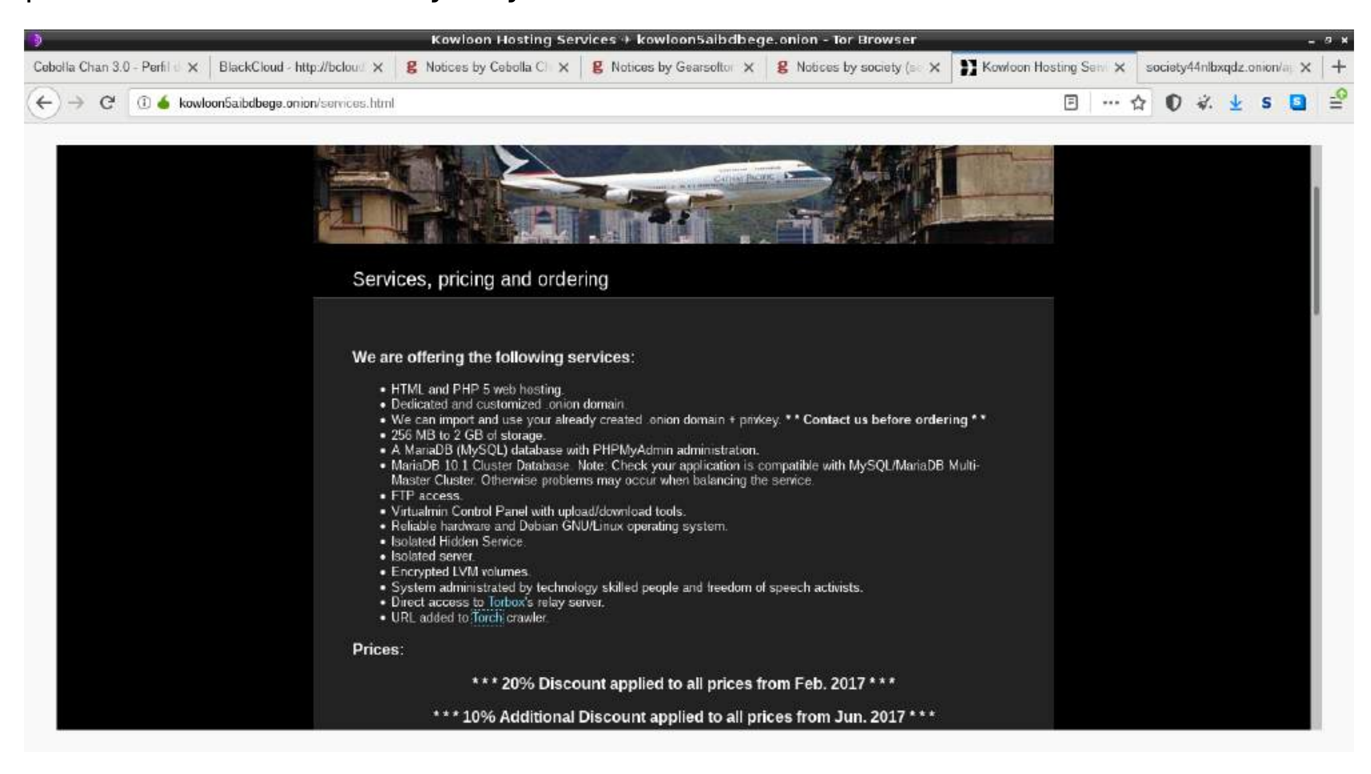
lulzwrzcle5ks3se.onion

bcloud2suoza3ybr.onion

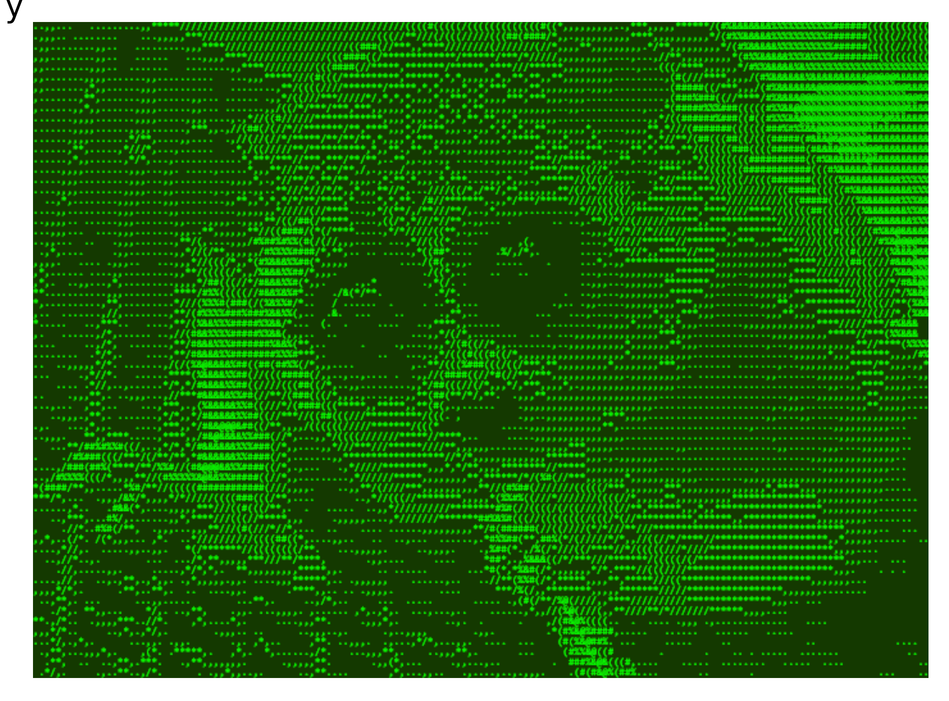
society44nlbxqdz.onion

kowloon5aibdbege.onion → Servicio de hosting

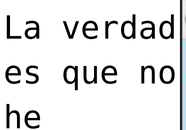
Mira que me interesó mucho el asunto, ya que por experiencia en el pasado suele existir una posibilidad que los sitios estén alojados en el mismo servidor, añadirle a ello que todos los sitios se publicitan entre sí y hay varias similaridades.



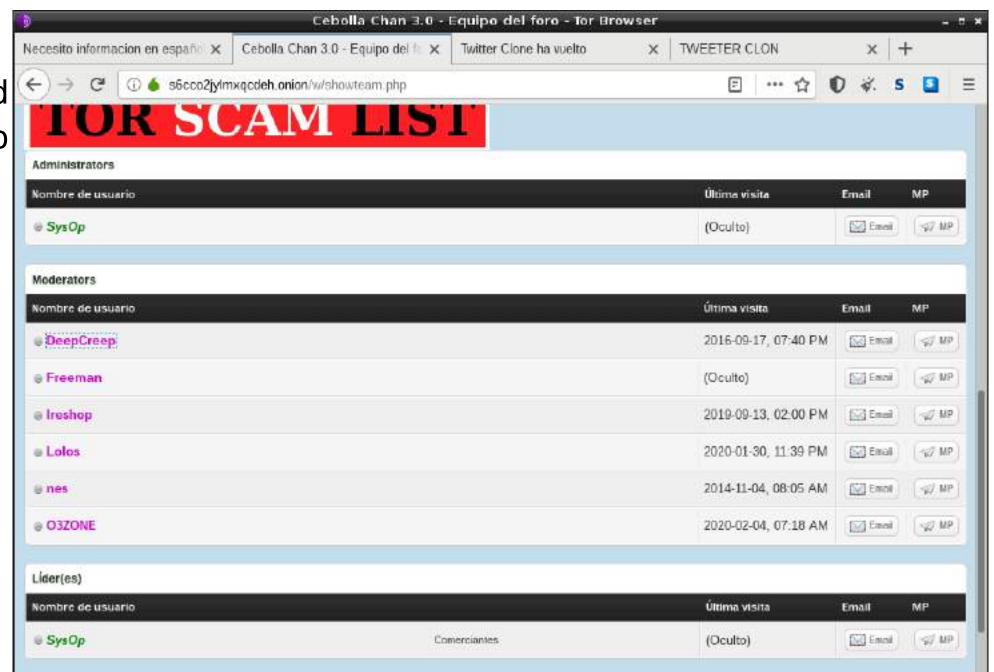
Además para confirmar mis sospechas he usado un software para hacer un ddos utilizando un ataque slowpost que satura el servidor de peticiones incompletas hasta que se estresa a tal punto que colapsa, dirigí un fork de slowloris usando tor como proxy hacia el foro cebolla chan y… Tadan! Los sitios anteriormente mencionados estaban caídos al mismo tiempo, incluyendo torbox, y si, accedí desde otra red para verificar ello y no fuera mi ancho de banda el saturado, si usted es parte de una agencia de inteligencia este es un paso que no deberían saltar.



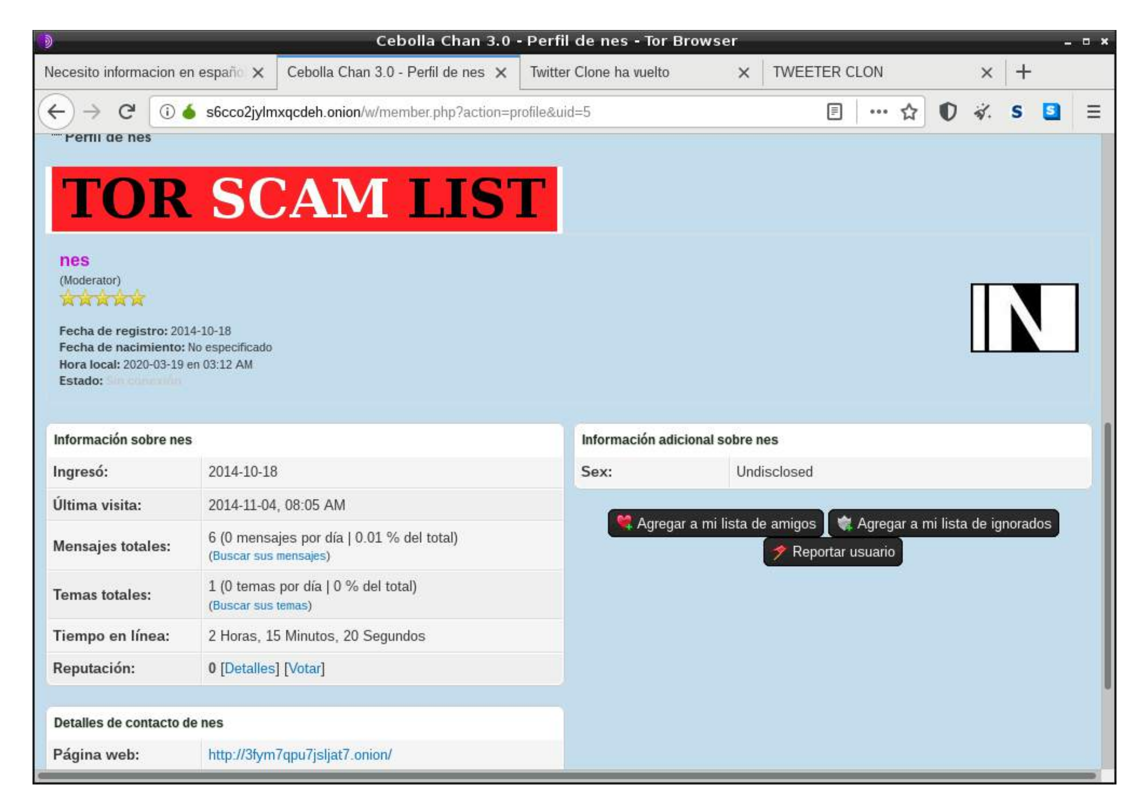
Ahora atacaré a lo principal, veamos a el grupo de administración del foro cebolla chan:



La verdad es que no he



encontrado nada de interés en la actividad de los otros usuarios, a excepción de “nes”.



Primera conexión en C.C: 18/10/2014

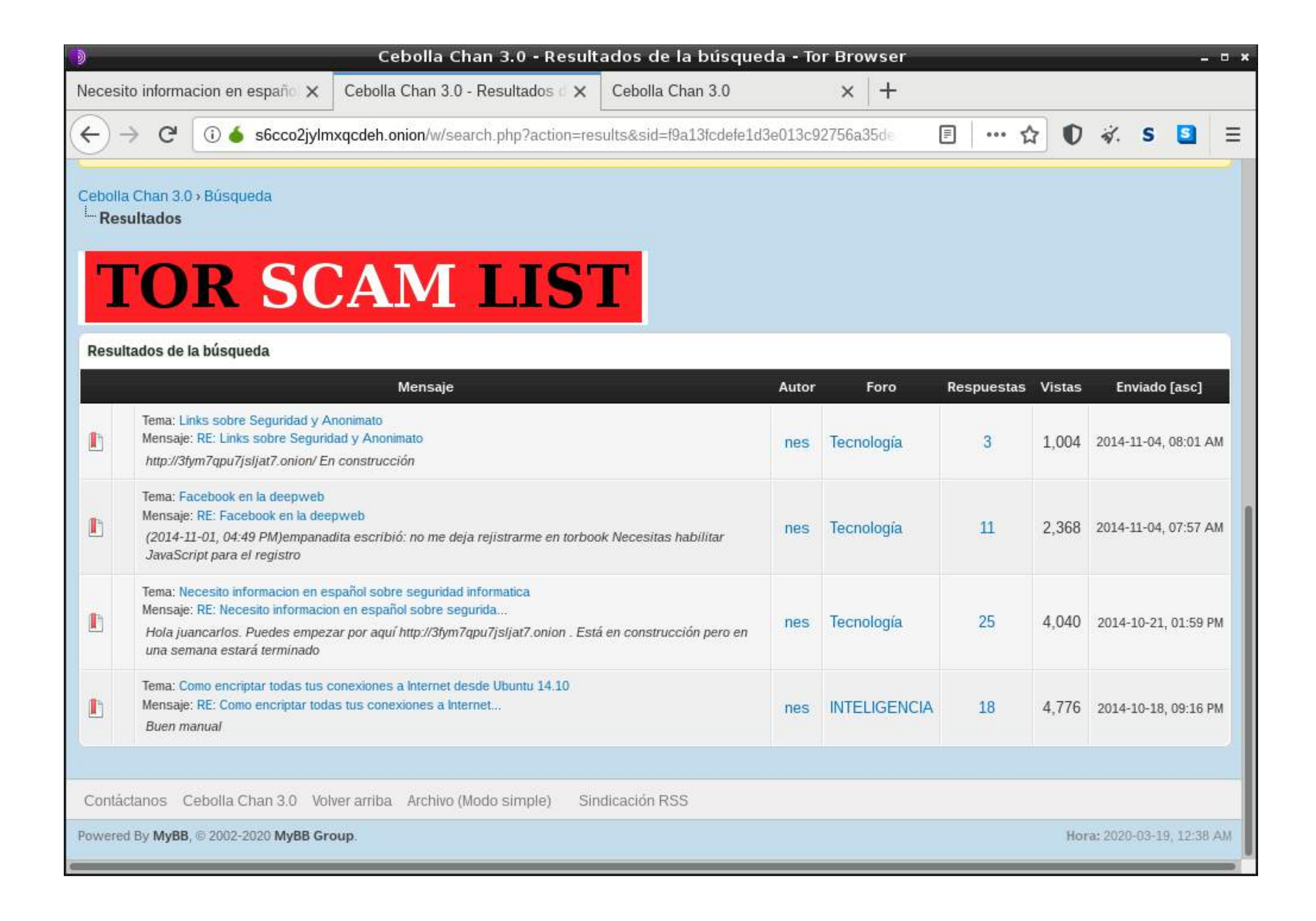
Última Conexión en C.C: 04/11/2014

Tiempo de existencia de cuenta: 2 semanas

De los primeros 5 usuarios de C.C: siendo el único inactivo no borrado

Conocido de SysOp(?)

Tiene algunos cuantos mensajes en las dos horas que estuvo en línea.



Desde su perfil de moderador hace alusión a cierto sitio (Que ya no existe) "Nes web" http://3fym7qpu7jsljat7.onion/, que era un sitio básico en html sin javascript con el que pretendía mostrar sus conocimientos sobre seguridad y anonimato en la red tor, gracias a la todopoderosa internet archive podemos ver lo que era:

https://archive.is/9Xwyc



De la primera vez que se tiene constancia de la existencia del sitio es desde 2014-10-21 según el post de el foro, después no se supo más de su creador ni del sitio, a la fecha sabemos que el sitio estaba alojado en el hosting de Freedom Hosting II que fué hackeado allá por 2017 y los hackers filtraron la base de datos y archivos de sistema, por lo cual pueden darse gusto buscando más info allí.

Lista de sitios en el hosting: https://pastebin.com/gRWYY9z4

Archivos de sistema: https://s3-eu-west-1.amazonaws.com/freedomhosting2/fhosting-system.tar.gz.torrent

Base de datos: https://s3-eu-west-1.amazonaws.com/freedomhosting2/fhosting.sql.gz.torrent

Lo que encontré con el comando grep es hermoso, he hallado la privatekey que me permite usar ese dominio .onion

3fym7qpu7jsljat7.onion

-----BEGIN RSA PRIVATE KEY-----

MIICXQIBAAKBgQCkSiMm7qayyjJE1UdW4gy+OWVLySC7QDh04mu4qnmRlKUdgYr9

g2oSlCbB+F4QROReLmsUICWUKHaZMw7AQQVyiD/YjDrtIpRdeZP5rESWAoWBMtpN

lexqTL55bgYCduSfw7/QNDJh3tAk7BZP9q9aNOaSKkUqs/V5Y+wpWCHyOwIDAQAB

AoGAYbQRabLeAlALSzJHpdzzVSGPI13ukE2mBaUuCPmhKLns5DpJLXE84OWokwyg

7C38XiJe3e4sSwsxVPSvXhiNItbz2qyMTHNJEpkUDqedAph8i6xfRP0Y+E3FcHgI

EQf8jeg4tWJpUt8/iHdPBONc5BDArsIZvsN5+90FlxwRchkCQQDR9PsUNqwc+5Oz

I9WbqowDhhgS/rY1pJW7i4TKbjTXgyVZkb9qbjqSuFXkcT+nT+oS32qYqSw658bb

mKu4n+kdAkEAyFFiIgmezOb8FmIc2uG2CxARHA4bGDn5okWTQQ7mQo20DZ1/5Z4n

aWXtcuHnmoxw+C0iwXFs+gmBK+7qdKjBNwJAL7sk9XR0bmZXLquf3TLJf+eVQ4Q6

gjl3fNp8BtVFGBWNgS5cOOL0V/SmOjfww6WsTjwSbMBQ+NdGYxfzOhbIlQJBALs2

5GIvX4zc7Aj3VURz4rFgKL1xqXzw4g/4unD5PdZBnV+ELX4qW2cz7cGKw+w7CXHI

rUzhdxoQO/sVZWX2Oe0CQQCMTNBboDozTElrK7YAZNge76kYsDR57akSmA2ig9Sw

RI4PAQxKLDuW4GBl50EhMWA9f3f3T2s7WviA0qYhwEot

-----END RSA PRIVATE KEY-----

En el sitio podemos observar ciertos detalles, entre ellos las direcciones bitcoin y litecoin:

BTC: 16P7LjXyijokEArDPERhG2k6d8EHBRqEhe



LTC: LiLaF1ZRL3K26PNv1fJjwoNYsHyH2GPX2V



Y un email de contacto: nes@mail2tor.com

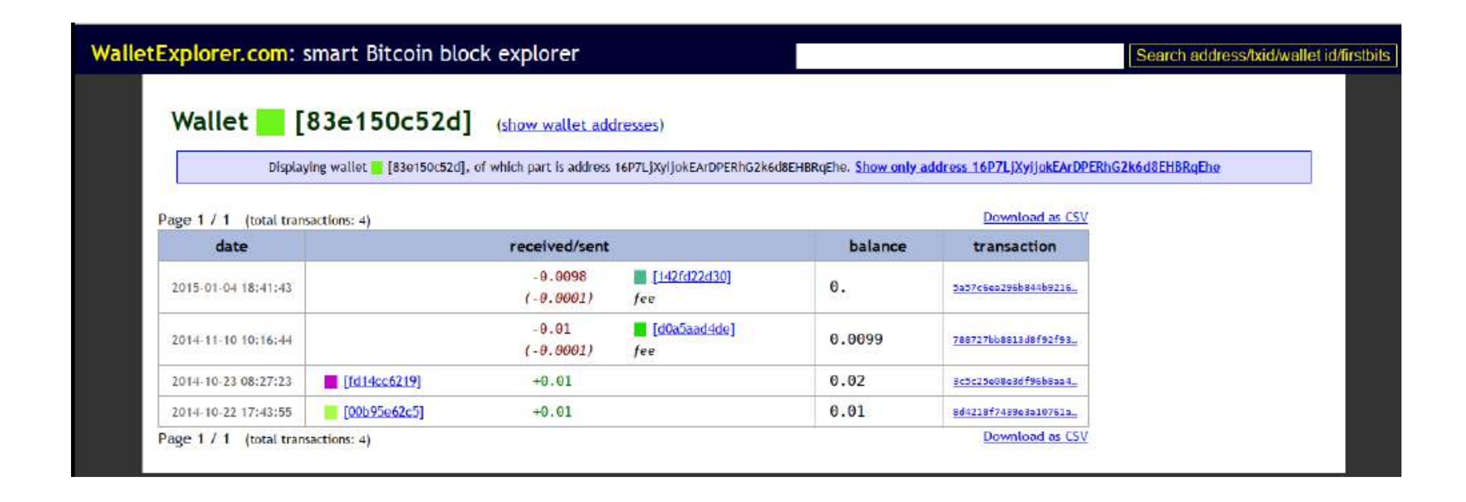
Primero veamos la actividad asociada a esa dirección bitcoin:

https://www.blockchain.com/es/btc/address/16P7LjXyijokEArDPERhG2k6d8EHBRqEhe



Ha hecho 4 transacciones y ha movido aproximadamente 0,02 bitcoin, lo que hoy sería 185 dólares.

https://www.walletexplorer.com/wallet/83e150c52d70f41e?from_address=16P7LjXyijokEArDPERhG2k6d8EHBRqEhe

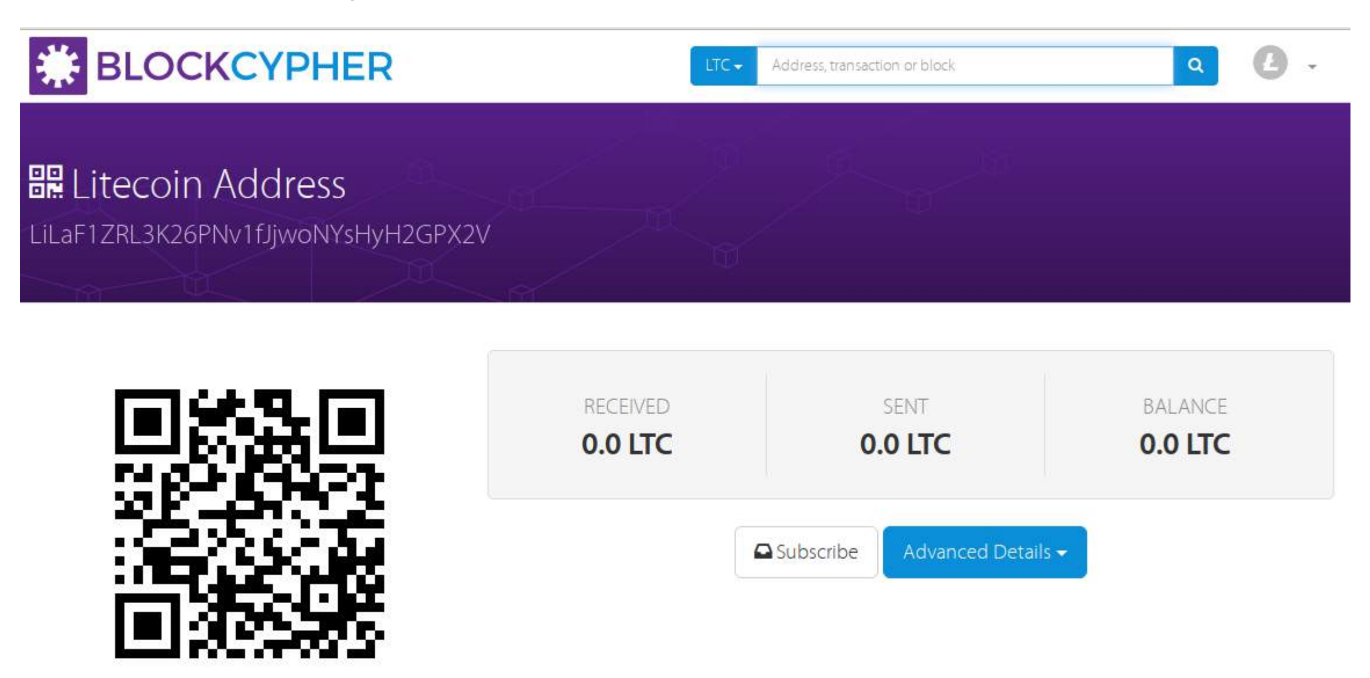


La última transacción fué el 4 de enero del 2015 y se ha hecho las siguientes transacciones en el transcurso de la vida de la dirección:

Movimiento	Monto	Dirección	Fecha
Recibido	0,01	15LqZnGqVYQwWgtpAecPMNjKU4xQsXCSuK	2014-10-22 11:43
Recibido	0,01	1Mmu6eP1JkXV8VaLabMqxYhd8LaiGiNqAZ	2014-10-23 02:27
Enviado	0,01	1LG2NDxz9GfqZYipYbGM5ie3jzfGNuGhYU	2014-11-10 04:16
Enviado	0,0098	1LBWrAaH7jwNFk2aTb8Zdbg86f2uQ2nsuc	2015-01-04 12:41

Esta información puede ser clave si trabajas para alguna agencia gubernamental y puedes consultar a diversos wallets en línea, exchanges y mixers por más información.

En Litecoin no hay nada :(



Revisando el correo de contacto que deja nes@mail2tor.com, usando herramientas como https://haveibeenpwned.com/ para ver si ha sido expuesto en algúna filtración de datos no me ha dado resultados, igualmente se pueden usar otras herramientas o recursos como https://dehashed.com/, https://intelx.io/ para consultar esto, ya que si por casualidad encontramos un email, nombre de usuario, número de teléfono y encontramos que existe información sensible filtrada podemos hacer uso de ella, en lo personal me gusta checar https://raidforums.com/ para buscar bases de datos.



También hice una búsqueda en google usando dorks, la cual fué infructosa: intext:”nes@mail2tor.com” :(

En fin, si eres parte de una agencia de gobierno según urlscan.io

https://urlscan.io/result/ed870b65-d58e-49c4-aaa0-bd236154e562

El servidor de mail2tor está ubicado en Noruega y hay posibilidades de que si escriben una nota legal pidiendo acceso a la data de el usuario, a lo mejor obtienen más información.

Sigamos…

Desde que comencé la labor ha pasado un buen tiempo, actualmente el sitio que hace correlación en la clearnet redirigue a google, por lo cual no aparecerá en las búsquedas del mismo ya, pero quiero que conste que usé la vieja confiable de intext:”3fym7qpu7jsljat7.onion” y rebusqué en los resultados, sin embargo tengo la suerte de tener al salvador bing que aún muestra el sitio entre sus resultados

Simplemente escribí la url en bing.com y me apareció un par de coincidencias en particular

1- https://www.bing.com/search?q=3fym7qpu7jsljat7.onion&qs=n&sp=-1&pq=3fym7qpu7jsljat7.onion&sc=0-22&sk=&cvid=91EF236D2BFD4DE0AAED85F1EB12DCEE&first=7&FORM=PERE

Dark Web Links For Hacking - Easy Onion | ... Traducir esta página
https://easyonion.com/dark-web-links-for-hacking
3fym7qpu7jsljat7.onion – Hacking – HackerLabs: When I checked this dark web links then not able to see any useful information on website webpage. Tags: browser for dark web dark web documentary dark web forums dark web porn sites dark web walkthrough dark web working links darkweblinks deep web links facebook hack hack.

2- https://www.bing.com/search?q=3fym7qpu7jsljat7.onion&qs=n&sp=-1&pq=3fym7qpu7jsljat7.onion&sc=0-22&sk=&cvid=91EF236D2BFD4DE0AAED85F1EB12DCEE&first=17&FORM=PERE1)

Trabaja en HackerLabs
https://hackerlabs.es/trabajo.html
¿Estás especializado en algún campo de la tecnología y buscas trabajo? Buscamos especialistas con ganas de aprender y trabar en equipo. Completa nuestros desafios en la red Tor para unirte a nosotros

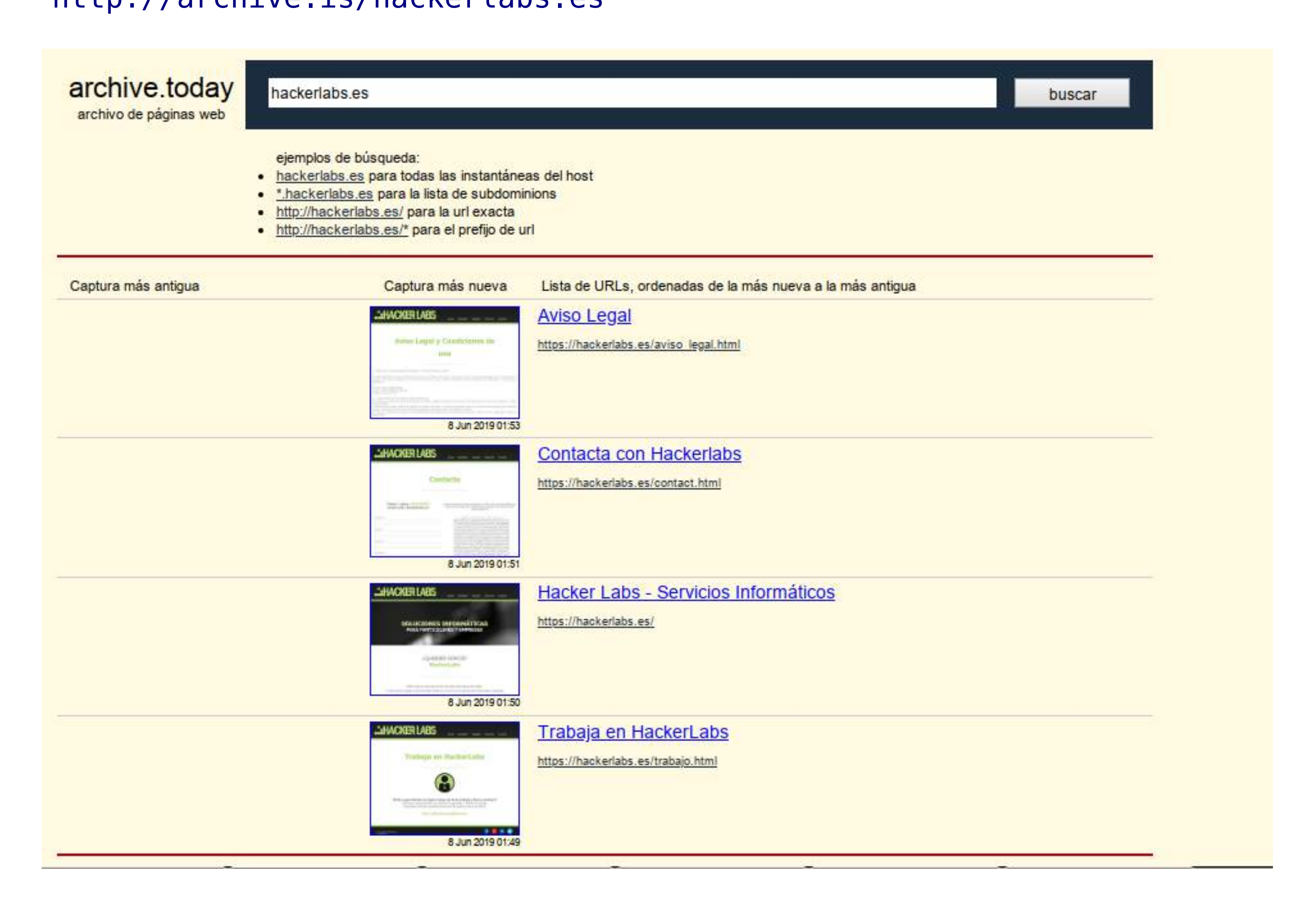
Ambos están guardados en la caché de bing:

1- https://cc.bingj.com/cache.aspx?q=3fym7qpu7jsljat7.onion&d=4792152857904213&mkt=es-XL&setlang=es-ES&w=dAoWS8qN50-DOCM-_Mx6MLoeTwAoSHKR

2- https://cc.bingj.com/cache.aspx?q=3fym7qpu7jsljat7.onion+hackerlabs&d=4773731737208201&mkt=es-XL&setlang=es-ES&w=d6RXxotM9EJ61_zwvvSIeaObyftCA_Xr

El primero hace alusión a “hackerlabs” texto que no aparece para nada en la versión guardada que tenemos del sitio en internet archive, seguido tenemos la aparición de un dominio “hackerlabs.es” que coincide con nuestro término de búsqueda.

La verdad es que ya tenía guardada previamente una versión del sitio en archive.is que pueden encontrar aquí en http://archive.is/hackerlabs.es



Observa la página del sitio en la que ofrecen trabajo:

http://archive.is/Eb7Bq

Trabaja en HackerLabs



¿Estás especializado en algún campo de la tecnología y buscas trabajo?
Buscamos especialistas con ganas de aprender y trabar en equipo
Completa nuestros desafios en la red Tor para unirte a nosotros

http://3fym7qpu7jsljat7.onion

Mira que bonito, nuestra url, aquí el administración de forma explícita acepta que el sitio es de su autoría, pero sigamos revisando el sitio…

La página principal: http://archive.is/s93lM

SOLUCIONES INFORMÁTICAS
PARA PARTICULARES Y EMPRESAS

¿QUIENES SOMOS?
HackerLabs

Hacker Labs es una empresa de soluciones informáticas de Madrid.
Con los mejores equipos y profesionales brindamos un servicio de soporte informático tanto a empresas como a particulares, en cualquier campo de la tecnología, con extraordinarios resultados en tiempo record.

Hum… una empresa de profesionales en tecnología… En Madrid…

¿Están seguros tus dispositivos móviles?
Así de fácil es hackear un teléfono



Mira que guay, hay un vídeo de la sexta en el cual explican lo fácil que es hackear un teléfono (Si consideran hackear instalarle un Rat a un teléfono teniendo acceso físico)

Link de la entrevista: https://www.lasexta.com/programas/equipo-investigacion/noticias/codificar-mensajes-whatsapp-protege-comunicaciones-hacker-muestra-vulnerabilidades-sistema_201612165854610d0cf20341e405f25a.html

El cuál según el pie de página se grabó en Madrid y está fechado el 12/11/2017, la entrevista la realiza Glòria Serra (https://es.wikipedia.org/wiki/Gl%C3%B2ria_Serra)

Si reproducimos el vídeo detenidamente podemos ver las fachadas de los negocios de los edificios al frente, luego podemos hacer una búsqueda en google map(O si conoces Madrid podrás saber dónde es en base a esto) descubrimos que El video fue grabado en Calle de Cedaceros con Carrera de S. Jerónimo, Madrid, España en el Edificio Número 34.

Además la hora en el movil marca las 13:17, 13:52 del sábado 8 de Noviembre del 2014.



Algo más?

Acaso no hay algo que estos chicos no puedan hacer? Entre ello **Hosting en la red Tor**, algo inusual para una pequeña "empresa" en la clearnet.

¿QUÉ OFRECEMOS?

SERVICIOS GENERALES

· Soporte técnico remoto y presencial
· Creación de nubes para empresas
· Recuperación de archivos borrados
· Optimización de sistemas operativos
· Restauración de sistemas y formateos completos
· Adaptaciones de páginas web a móviles
· Diseño de páginas web
· Hosting (con ssh y ftp)
· Instalación de drivers y periféricos
· Creación de programas a medida
· Community management

SEGURIDAD y HACKING

· Configuración de redes
· Eliminación de virus y programas espía
· Copias de seguridad en nuestros servidores
· Análisis de vulnerabilidades (pcs y webs)
· Hosting en la red Tor
· Sistemas de cifrado de datos
· Recuperación de contraseñas
· Monitorizacion de equipos
· Análisis y captura del tráfico de red
· Anonimato en Internet
· Prevención y reparación de ataques DDoS

¿No encuentras algo?
Contacta con nosotros, seguro que tenemos la solución.

SOPORTE TÉCNICO PARA EMPRESAS

Tenemos dos secciones interesantes que analizaremos más adelante, las cuales son contacto y el aviso legal.

Contacto: http://archive.is/PmFEH

Aviso legal: http://archive.is/f2E4K

Contacto

Néstor Muñoz - 655266553
nestor.mb@hackerlabs.es

Ciframos todos nuestros mensajes con SSL, pero puedes añadir una capa más de seguridad codificando tu mensaje con nuestra clave pública de PGP

Nombre *

Email *

Asunto *

Mensaje *

-----BEGIN PGP PUBLIC KEY BLOCK-----
-----END PGP PUBLIC KEY BLOCK-----

HACKER LABS

INICIO SERVICIOS TRABAJO CONTACTO CLIENTES

Aviso Legal y Condiciones de uso

I.- TÉRMINOS Y CONDICIONES DE ACCESO Y UTILIZACION DE LA WEB

En este apartado se incluye información sobre las condiciones de acceso y utilización de este sitio Web que deben ser conocidas por el usuario. Información necesaria a los efectos previstos en la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico.

•Titular: Néstor Muñoz Berzal
E-mail: nestor.mb@hackerlabs.es
Teléfono: 655 26 65 53

Ouch, ya tenemos tanta información.

Email: nestor.mb@hackerlabs.es (Busqué y no encontré ninguna correlación en otra parte)

Teléfono: 655 26 65 53 (Sin correlaciones)

Clave PGP (Sin correlaciones)

Nombre del titular: Nestor Muñóz Berzal.



Y aquí es adonde quería llegar!

El nick Nes en el foro Cebolla Chan y en Nes Web es tan sólo un juego de letras para el nombre real **Nestor**, al parecer al inicio del foro este individuo no se preocupó mucho por cuidar su OpSec, a pesar de que sabía muchas cosas sobre tecnología, a partir de aquí trataremos de conseguir más información de él y sus actividades.



Sigamos revisando en el sitio, o mejor dicho en la caché de bing…

En el sitio se ve que ofrecían un curso de hacking presencial, veamos:

https://cc.bingj.com/cache.aspx?q=hackerlabs.es&d=4606726233919028&mkt=es-XL&setlang=es-ES&w=_q0M7qJzHfcu5ZQUmbvOoRE8VPyggZfU

Duración: 40 horas

Periodo: Febrero, Marzo y Abril de 2017

Horario: Martes y Jueves 17h-21h

Coste: 450€

C\ Santa Virgilia nº19 Madrid (barrio Hortaleza)

Bonita dirección hermano, un poco caro para mi gusto, vamos a ubicar esto en un mapa:

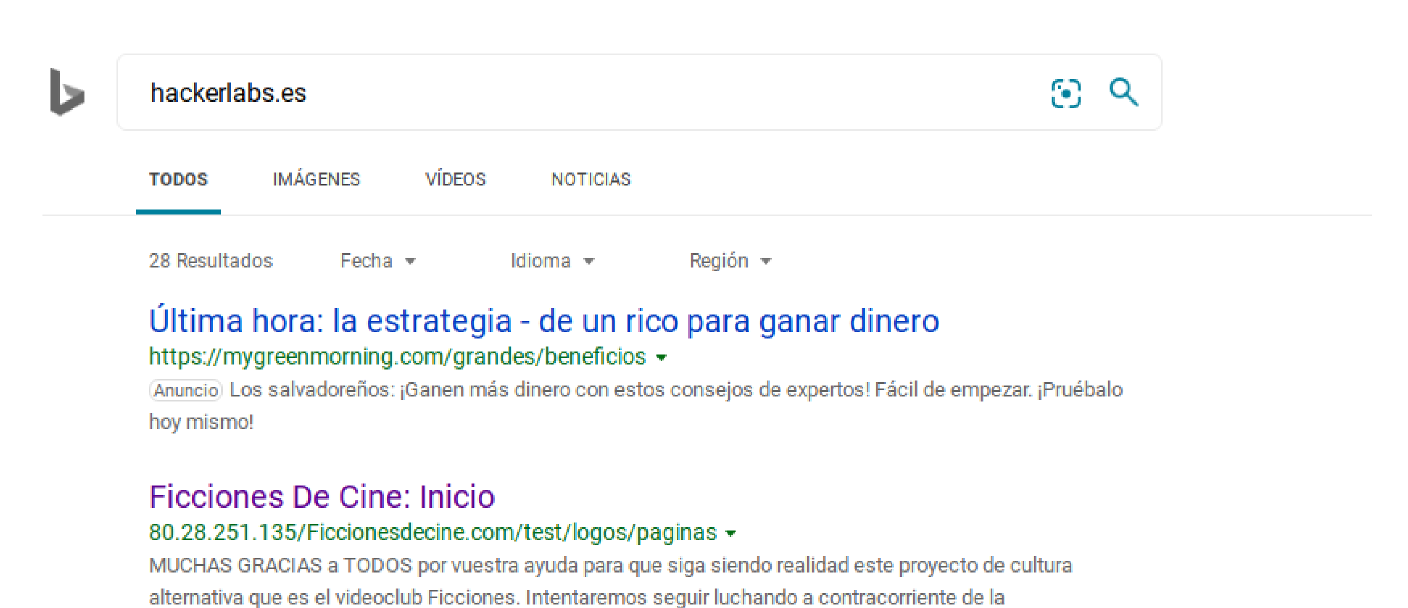


Excelente, ahora en Street view:

https://www.google.com/maps/@40.4258806,-3.705026,3a,75y,224.09h,88.93t/data=!3m6!1e1!3m4!1si_HtXJ0s7COJRT_Hu1-K8A!2e0!7i16384!8i8192



Ficciones? Un club dvd? No veo ningún letrero de hackerlabs por aquí, vamos a indagar…



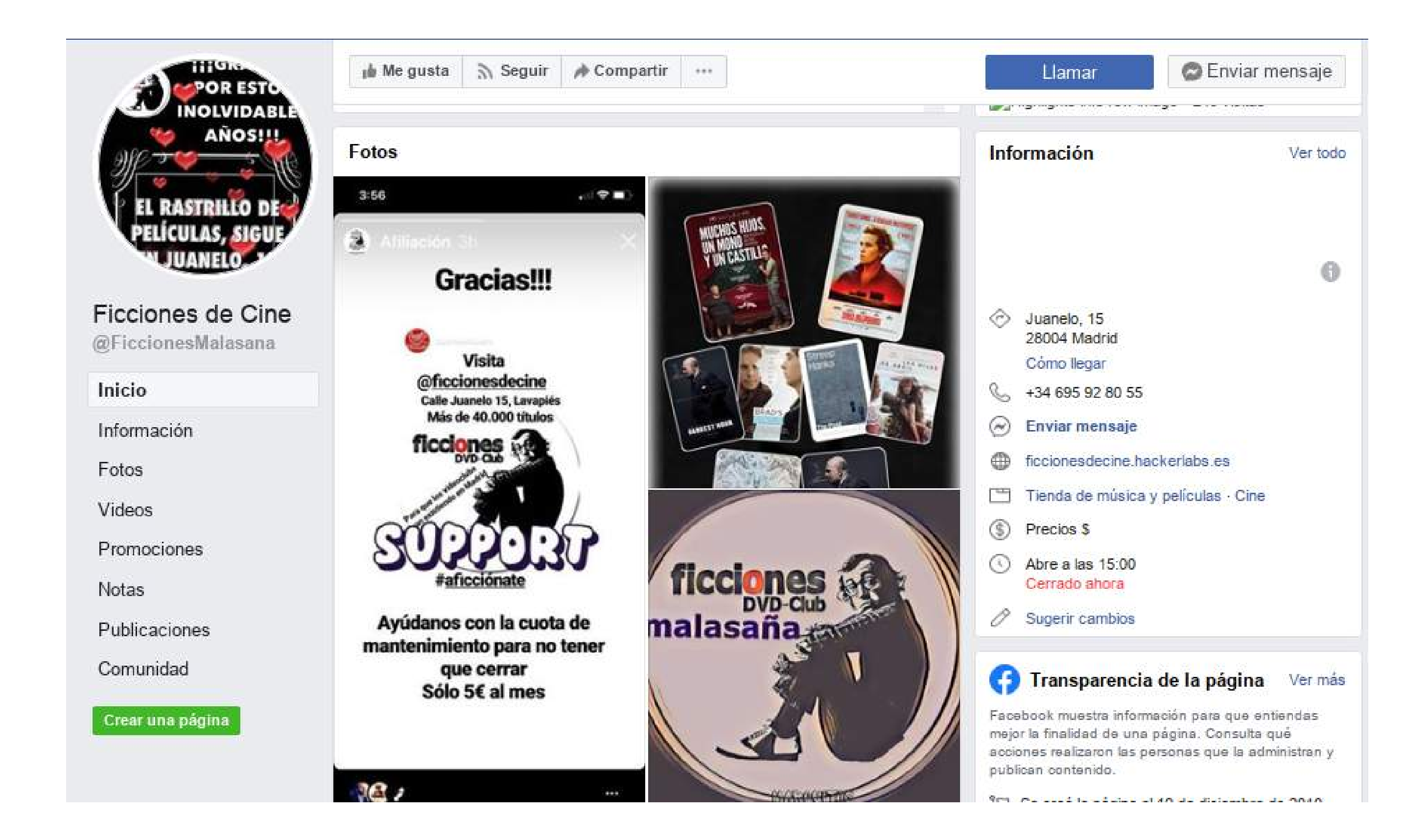
Seguimos con la coincidencia…



http://80.28.251.135/Ficcionesdecine.com/test/logos/paginas/index2.php

Ahora vamos a ver la página de facebook:

https://www.facebook.com/FiccionesMalasana/



Mirad en el apartado sitio web, es un subdominio de hackerlabs.es:

http://ficcionesdecine.hackerlabs.es/

Not Found

The requested URL was not found on this server.

Que no dirige a nada, sin embargo seguimos encontrando coincidencias en la web:

Ficciones De Cine
Alquiler de pelicula en Madrid

Detalles de la empresa Ficciones De Cine en Madrid.

Detalles de contacto

Categoría: Alquiler de pelicula

Número de teléfono: +34 913 69 33 1

Comunidad autónoma: Madrid

Ciudad: Madrid

Dirección: Calle Juanelo, 15, 28012 Madrid, Spain, Madrid, Madrid, 28012

Código postal: 28012

URL: http://ficcionesdecine.hackerlabs.es/

Editar informacion

¿Eres el dueño o representante de Ficciones De Cine?

Si la información sobre la empresa es incorrecta, puede editarla.

=>> Editar

https://madrid-madrid.empresas-espana.es/alquiler-de-pelicula/ficciones-de-cine-madrid/

En google también hay muchas referencias a la web, pero no pude recuperar ninguna captura del subdominio, mi hipótesis es que Nestor ofreció sus servicios de informático al diseñar la web y a la empresa de renta de dvds le pareció, pero el sitio se alojó temporalmente apuntando a su dominio principal.

m.yelp.ca › Shopping › Books, Mags, Music & Video › Music & DVDs
Ficciones de Cine - Music & DVDs - Calle de Juanelo ... - Yelp
Ficciones de Cine in Madrid, reviews by real people. Yelp is a fun and easy way to find, ... Call Now · Visit Website. http://ficcionesdecine.hackerlabs.es ...

www.yelp.com › ... › Books, Mags, Music & Video › Music & DVDs
Ficciones de Cine - Music & DVDs - Calle de Juanelo, 15 ...
Ficciones de Cine in Madrid, reviews by real people. Yelp is a fun and easy way to find, ... Call Now · Visit Website. http://ficcionesdecine.hackerlabs.es ...

www.findglocal.com › España › Madrid › Empresas
Ficciones de Cine - Find Local Businesses
... la piratería http://play.cadenaser.com/audio/001RD010000005709014?autoplay=true ... Renovamos el stock de camisetas en @ficcionesdecine !!! Ve por la ...

www.cineplo.com › España › Madrid
Ficciones de Cine - Juanelo, 15, Juanelo, nº 15 ... - Cineplo
http://play.cadenaser.com/audio/001RD010000005709014?autoplay=true. Hablamos con Marcia Seburo ... Renovamos el stock de camisetas en @ficcionesdecine !!! Ve por la tuya y de paso te ... Página web. ficcionesdecine.hackerlabs.es ...

www.cineplo.com › España › Madrid
Ficciones de Cine, Juanelo, 15, Madrid (2020) - Cineplo
... videoclub que resiste a la piratería http://play.cadenaser.com/audio/001RD010000005709014?autoplay=true. #HorarioDeVerano en Ficciones de Cine - Juanelo, 15 ¡Y no olvidéis seguirnos en ... Página web. ficcionesdecine.hackerlabs.es ...

madrid.empresasespanolas.net › Madrid › Madrid
FICCIONES DE CINE - Alquiler de peliculas - Calle de ...
Información completa sobre FICCIONES DE CINE em Madrid: Calle de Juanelo, 15, 28012 Madrid, España. Opiniones ... http://ficcionesdecine.hackerlabs.es/.

Para empezar quiero decir que por todos los medios posibles traté de buscar algún nexo con el número en el sitio y no encontré nada, ni en whatsapp, instagram, facebook, twitter, etc.

Lo único que se sabe es la compañía a la que está/estaba registrado el número (655 266 553), Orange.

https://ardilla.ai/



Como no dió resultados el análisis del número de teléfono vamos a revisar la información de whois que podemos consultar de forma gratuita y abierta en https://www.dominios.es/dominios/



Información de Dominio

Volver

Los datos de contacto de este dominio están ocultos. Si desea comunicarse con el Titular y el PCA pulse aquí

DATOS DEL TITULAR

Nombre del Dominio	hackerlabs.es
Estado	Activado
Identificador	C3E30C-ESNIC-F5
Titular	Nestor Munoz
Fecha de Alta	04-10-2015
Fecha de Caducidad	04-10-2019
Agente Registrador	ASCIO TECHNOLOGIES INC

PERSONA DE CONTACTO ADMINISTRATIVO

Identificador	**C3E30C-ESNIC-F5**
Nombre	**Nestor Munoz**

PERSONA DE CONTACTO TECNICO

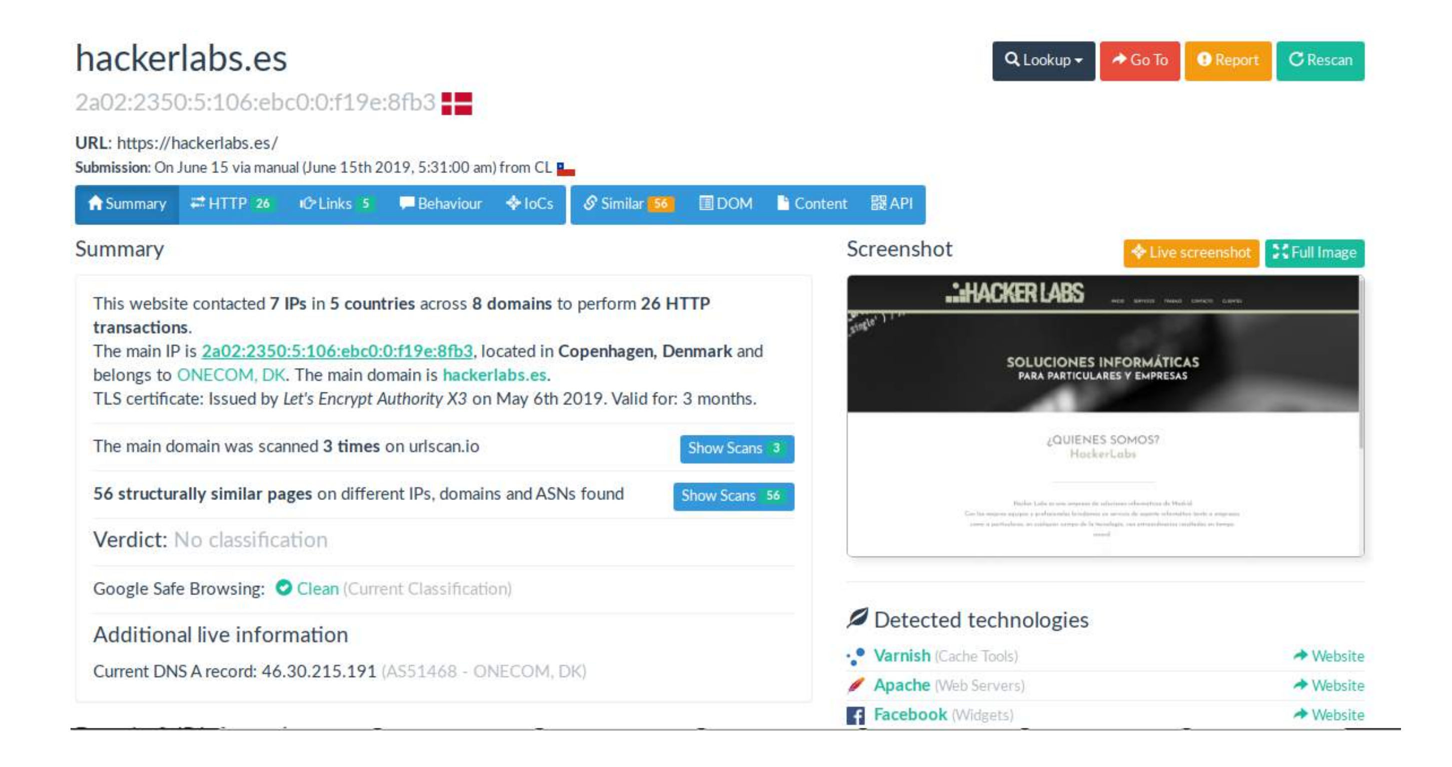
Identificador	**B74B7F-ESNIC-F5**

SERVIDORES DNS

Nombre Servidor	**IP**
ns01.one.com	
ns02.one.com	

Bueno, podemos notar que el sitio está registrado desde el cuatro de octubre del 2019 y que su registrador es Nestor Muñoz y el servidor dns está bajo la tutela de one.com que es una empresa localizada en Copenague. Dinamarca, veamos la data disponible en https://urlscan.io/:

https://urlscan.io/result/737aa423-3997-4954-b01d-fa6ad1bf1ebb/

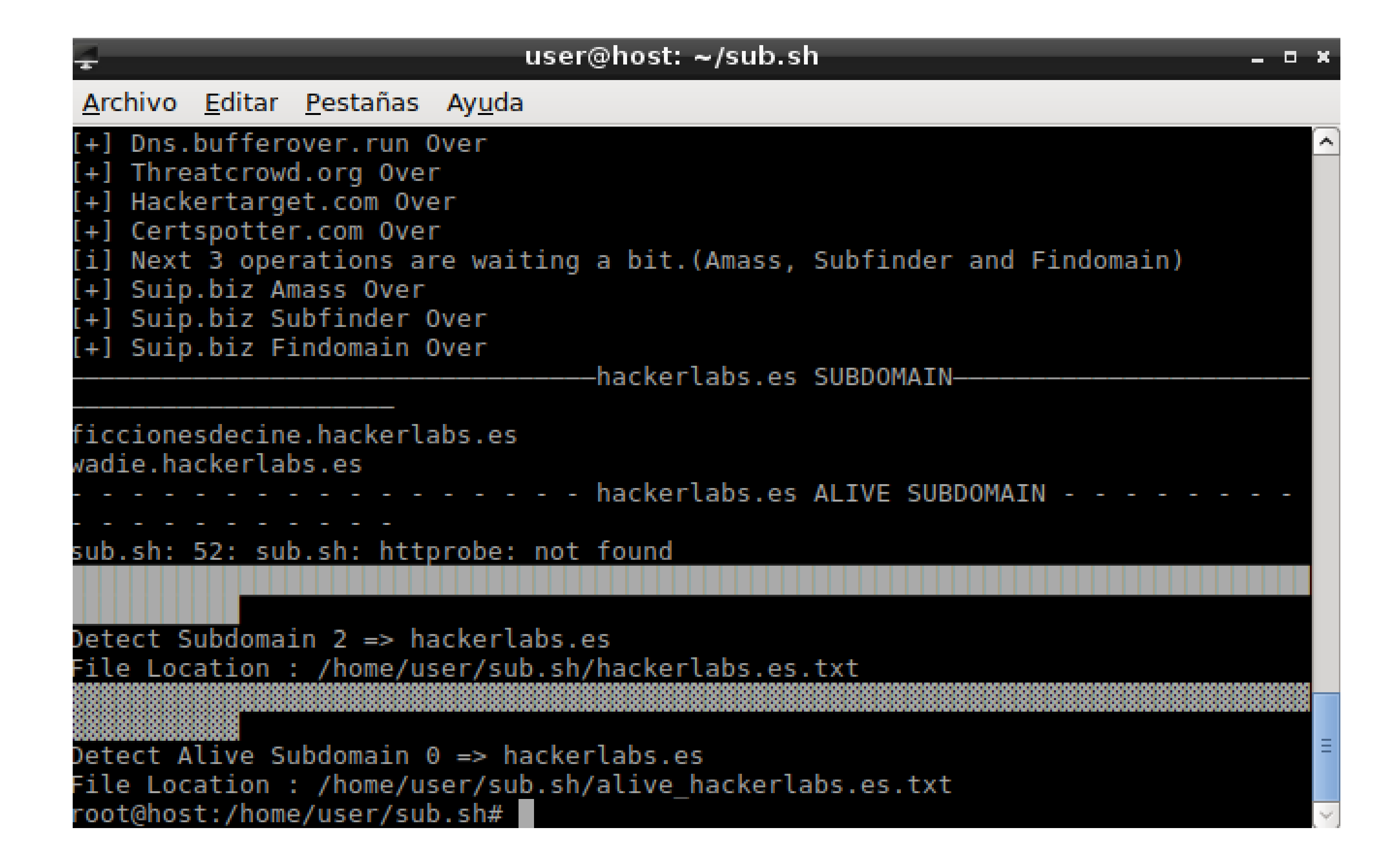


Bueno, ya saben a quien llamar pidiendo datos del usuario…



Usé cierta herramienta llamada sub.sh que sirve para buscar subdominios en el dominio y ver si encontramos más información: https://github.com/cihanmehmet/sub.sh

Fácil descargamos la herramienta y lanzamos el script: sh sub.sh hackerlabs.es



Tenemos dos subdominios vivos:

ficcionesdecine.hackerlabs.es

wadiehackerlabs.es

Sin embargo en ninguno de ellos hay algo de interés, sigamos.

Vamos a google a buscar más información sobre Nestor, probemos suerte escribiendo Muñoz Berzal Nestor, estos resultados llaman mi atención:

www.patentes-y-marcas.com › marca › pinganillo-nes-m3551605

PINGANILLO NES - Información sobre la marca

... sobre marcas, patentes y diseños. Esta marca ha sido solicitada por **NESTOR MUÑOZ BERZAL** a través del representante ÁLVARO HERRERA DÁVILA.

https://www.patentes-y-marcas.com/marca/pinganillo-nes-m3551605

www.madrid.org › Satellite › pdf PDF

Nº Resolución: 5268 ORDEN DE LA CONSEJERA DE ...

17 nov. 2017 - **MUÑOZ BERZAL NESTOR**. 15. 05-APC1-05723.3/2017. 05451001R. REYES LAYZA NANCY GRACIELA. 15. 05-APC1-02947.5/2017.

http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=filename%3DOrden+de+Resoluci%C3%B3n+inadmisi%C3%B3n+2017+-+5268.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1352942903388&ssbinary=true

Mira que interesante, primero tenemos una patente a su nombre, veamos:



Los productos y servicios protegidos por esta marca son:
09 - APARATOS E INSTRUMENTOS CIENTIFICOS, NAUTICOS, GEODESICOS, FOTOGRAFICOS, CINEMATOGRAFICOS, OPTICOS, DE PASAJE, DE MEDICION, DE SEÑALIZACION, DE CONTROL (INSPECCION), DE SALVAMENTO Y ENSEÑANZA, APARATOS E NSTRUMENTOS DE CONDUCCION, DISTRIBUCION, TRANSFORMACION, ACUMULACION, REGULACION O CONTROL DE LA ELECTRICIDAD, APARATOS DE GRABACION, TRANSMISION O REPRODUCCION DE SONIDO O IMAGENES; SOPORTES DE REGISTROS MAGNETICOS, DISCOS ACUSTICOS, DISCOS COMPACTOS, DVD Y OTROS SOPORTES DE GRABACION DIGITALES; MECANISMOS PARA APARATOS DE PREVIO PAGO, CAJAS REGISTRADORAS, MAQUINAS DE CALCULAR, EQUIPOS DE PROCESAMIENTO DE DATOS, ORDENADORES, SOFTWARE, EXTINTORES.
- Clases limitadas y modificadas:
09 - APARATOS PARA EL REGISTRO, TRANSMISION O REPRODUCCION DEL SONIDO.

En fecha 10/03/2015 se realizó COMUNICACION A TITULARES DERECHOS ANTERIORES (ART.18,4LM): M2579589
En fecha 16/03/2015 se realizó PUBLICACION DE SOLICITUD
En fecha 08/04/2015 se realizó OPOSICION DE LA MARCA 2579589 CLASES OPONENTES: 09
En fecha 08/04/2015 se realizó OPOSICION DE LA MARCA 2754708 CLASES OPONENTES: 38
En fecha 08/04/2015 se realizó OPOSICION DE LA MARCA 2789206 CLASES OPONENTES: 35
En fecha 08/04/2015 se realizó OPOSICION DE LA MARCA 2976930 CLASES OPONENTES: 09
En fecha 07/07/2015 se realizó PUBL.SUSPENSO FONDO DE F.RESOL 01/07/2015CAUSAS DEL SUSPENSO DE FONDO: 346
En fecha 27/07/2015 se realizó PERSONACION AGENTE
En fecha 29/07/2015 se realizó CONTESTACION AL SUSPENSO PUBLICADO EL: 07/07/2015
En fecha 25/09/2015 se realizó PUBLIC. DENEGACION DE F.RESOL: 21/09/2015

País: España

Fecha de solicitud: 06/03/2015

Número solicitud:
M3551605(4)

Datos del titular:
NESTOR MUÑOZ BERZAL

Datos del representante:
Álvaro Herrera Dávila

Tipo de registro: Mixta

El 6 de marzo de 2015 Nestor Muñoz Berzal solicitó el registro de una marca “Pinganillo NES”, pero a todo esto ¿Qué es un Pinganillo?



Según blogscvc.cervantes.es es un aparato intercomunicador compuesto de un pequeño auricular que se coloca dentro de la oreja y un receptor con cable o inalámbrico, que se emplea como sistema de comunicación por periodistas, deportistas y otros profesionales, ya que por su escaso tamaño es discreto y no dificulta la movilidad.

A Nestor le gusta dejar Nes en todos lados como firma personal al parecer, todo muy bien pero no parece haber ninguna otra referencia a la marca en la web, al parecer no tuvo tanto éxito nuestro amigo emprendedor, sigamos con nuestra búsqueda.

Este es un documento oficial del gobierno de Madrid, aquí hay información importante:

http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=filename%3DOrden+de+Resoluci%C3%B3n+inadmisi%C3%B3n+2017+-+5268.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1352942903388&ssbinary=true

05-APC1-03491.7/2017	05450244A	MUÑOZ BERZAL NESTOR	15

Tener tu DNI expuesto en internet no parece muy privado,

Podemos hacer algunas cosas en internet con su número, busquemos que hayamos de bueno en google con: 05450244A

Al parecer le denegaron unas solicitudes de trabajo (04/06/2010):

http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1271611120380&ssbinary=true



Area de Planificación y Desarrollo
Dirección de Recursos Humanos
04/06/2010

LISTADO PROVISIONAL DE ASPIRANTES ADMITIDOS, NO ADMITIDOS Y EXCLUIDOS A LA BOLSA DE TRABAJO DE CONTRATACIÓN TEMPORAL.

PUESTOS DE TRABAJO: TELEFONISTA-RECEPCIONISTA

PLAZO DE RECLAMACIONES DESDE EL 5 AL 14 DE JUNIO DE 2010 (AMBOS INCLUSIVE), de 9 a 14 horas

Las reclamaciones deberán dirigirse a: Dirección Gerencia del Hospital Universitario de Fuenlabrada, Camino del Molino 2,28942 Fuenlabrada

05450244A	Muñoz	Berzal	Nestor	0,5	No Admitido	Falta certificado vida laboral. Falta certificado servicios prestados.

Más…



Area de Planificación y Desarrollo
Dirección de Recursos Humanos
04/06/2010

LISTADO PROVISIONAL DE ASPIRANTES ADMITIDOS, NO ADMITIDOS Y EXCLUIDOS A LA BOLSA DE TRABAJO DE CONTRATACIÓN TEMPORAL.

PUESTO DE TRABAJO: AUXILIAR ADMINISTRATIVO

PLAZO DE RECLAMACIONES DESDE EL 5 AL 14 DE JUNIO DE 2010 (AMBOS INCLUSIVE), de 9 a 14 horas

Las reclamaciones deberán dirigirse a: Dirección Gerencia del Hospital Universitario de Fuenlabrada, Camino del Molino 2,28942 Fuenlabrada

05450244A	Muñoz	Berzal	Nestor	0,5	No Admitido	Falta certificado vida laboral. Falta certificado servicios prestados.

Y más adelante podemos observar unos documentos de la universidad complutense de Madrid, del grado de ingeniería en comunicaciones(10/2018):

https://fisicas.ucm.es/data/cont/docs/18-2018-10-10-Lista_Asignaci%C3%B3n_TFG_IEC_2018.pdf

https://fisicas.ucm.es/data/cont/docs/18-2018-10-03-ListaprelacionTFG_gradoIEC_2018-19.pdf

Alumnos excluidos

- 53567098Y
- 05450244A

Ahora vamos a ver en facebook:



Simplemente podemos ir insertando los datos que ya tenemos, en mi caso ya me aparece gracias al algoritmo de facebook (Gracias Suckenberg), tenemos detalles como que ha vivido o vive en Madrid, que ha estudiado en la Universidad Complutense de Madrid, apellidos, en mi caso tuve que ir probando con varias combinaciones hasta dar con él, por aguna razón al igual que muchas otras personas aquí usa un apellido diferente.

https://www.facebook.com/nehstor



Tenemos esta completa presentación:

Detalles

Trabaja en Hacker Labs

Estudió Ingeniería Electrónica de Telecomunicaciones en Universidad Complutense de Madrid

Estudió en Conservatorio Profesional de Música Teresa Berganza

Estudió en San Isidro

Estudió en San Viator

Vive en Madrid

De Madrid

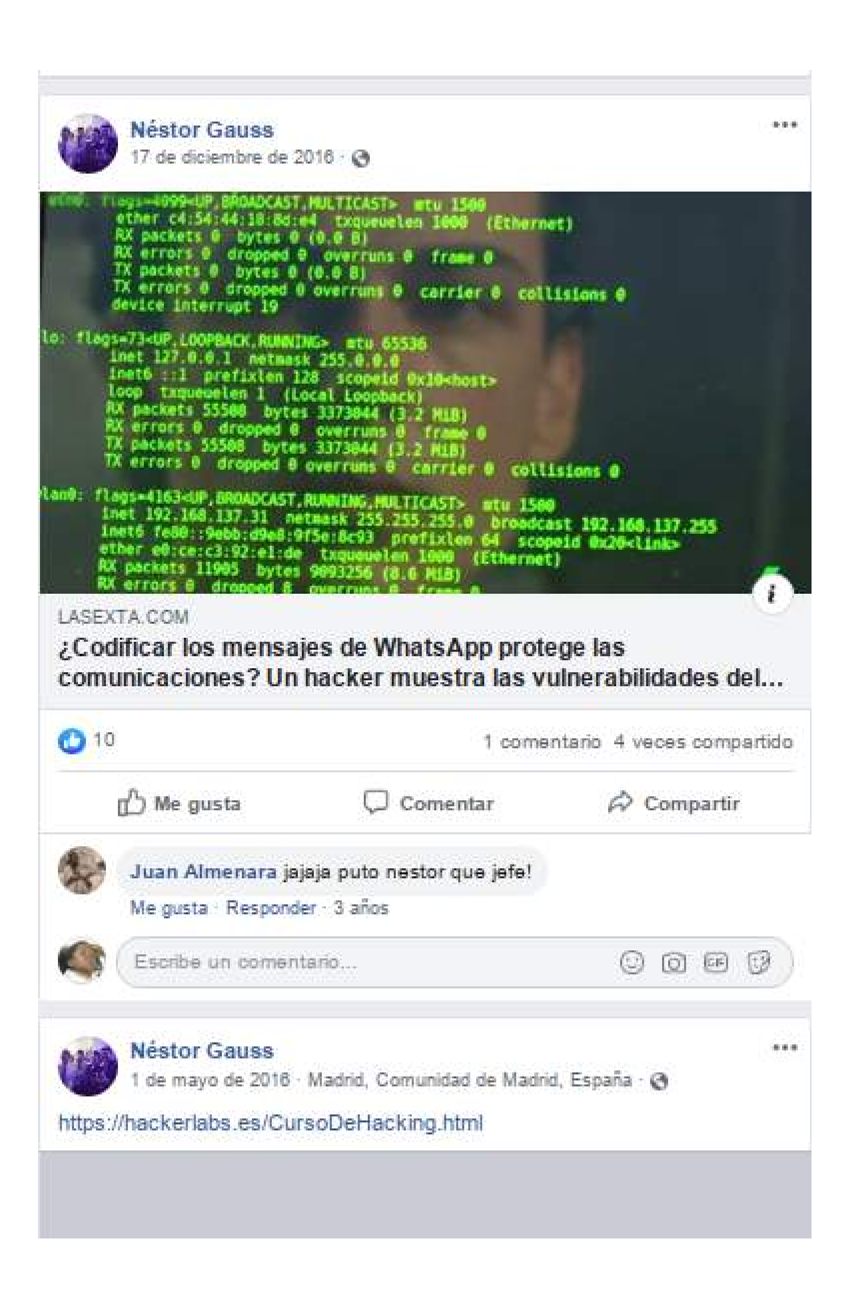
Foto de Nestor:



En su perfil encontré varios datos datos privados que me parecieron muy poco relevantes, pero entre algunas cosas que puedo destacar es que su lista de amigos está oculta, además que su última actividad pública fué el 30 de diciembre de 2017 en su perfil de facebook:



Además de unas publicaciones sobre su entrevista para la sexta y su curso de hacking de hackerlabs.es

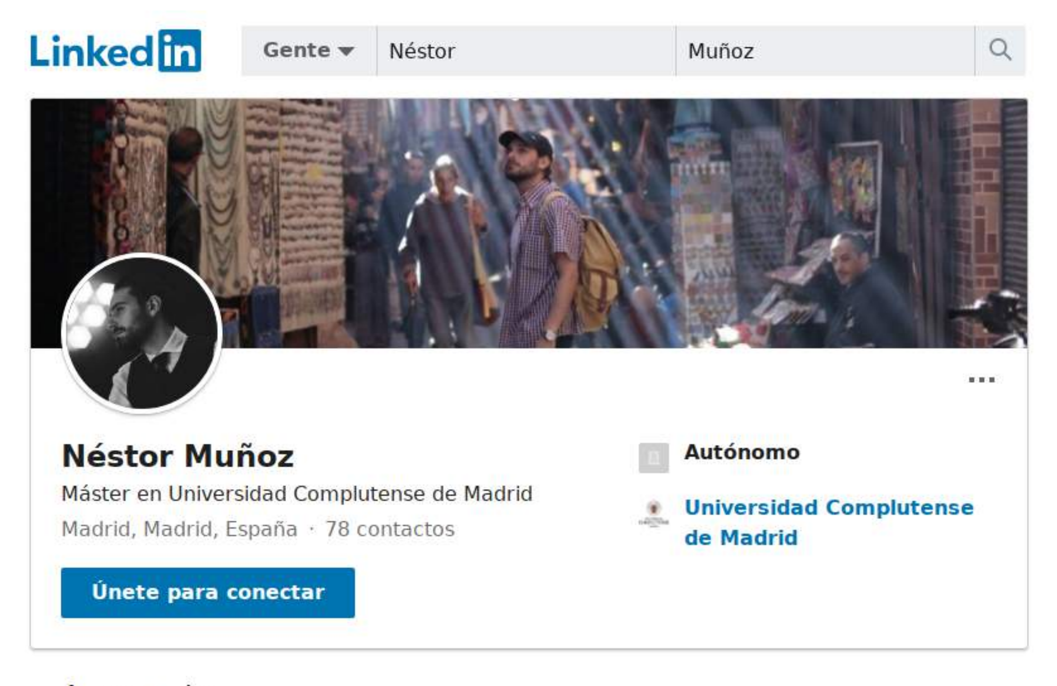


Néstor Gauss
17 de diciembre de 2016 ·
LASEXTA.COM
¿Codificar los mensajes de WhatsApp protege las comunicaciones? Un hacker muestra las vulnerabilidades del...
10
1 comentario 4 veces compartido
Me gusta
Comentar
Compartir
Juan Almenara jajaja puto nestor que jefe!
Me gusta · Responder · 3 años
Escribe un comentario...
Néstor Gauss
1 de mayo de 2016 · Madrid, Comunidad de Madrid, España ·
https://hackerlabs.es/CursoDeHacking.html

Tenemos la página de facebook de hackerlabs, cuyas primeras y últimas actividades fueron el 8 de abril de 2018



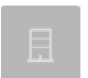
Claro que se pueden conseguir más datos sobre sus amigos y familia en facebook, pero dejaremos esto hasta allí, buscando en linkedin encontramos su perfil: https://es.linkedin.com/in/nesmunoz



Acerca de

Fotografía. Viajar. Vivir. Actualmente construyendo mi propio blog de viajes.

Experiencia



Fotógrafo autónomo
Autónomo
2013 – Actualidad · 7 años
Guadalajara y alrededores, España
Realizo diversos trabajos de reportaje gráfico para uso doméstico (familias, niños, pre-boda...) así como para personas que comienzan en el mundo de la moda y necesitan un book.



Fotógrafo
Guadaqué
sept. de 2015 – sept. de 2018 · 3 años 1 mes
Guadalajara y alrededores, España
Fotógrafo para el periódico Guadaqué que cubre la provincia de Guadalajara.



Barman
Cubana Waterloo Ltd
jun. de 2017 – sept. de 2017 · 4 meses
London, Reino Unido

Educación

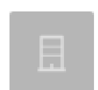


Universidad Complutense de Madrid
Máster · Análisis Sociocultural
2018 – 2019
Análisis Sociocultural del Conocimiento y de la Comunicación



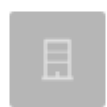
Universidad Complutense de Madrid
Comunicación Audiovisual · Comunicación audiovisual
2014 – 2018

Experiencia de voluntariado

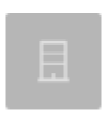


Director
Corto documental con Acción Social por la Música
abr. de 2018 – jun. de 2018 · 3 meses
Infancia
Lo que empezó como un pequeño proyecto acabó convirtiéndose en un corto documental para una asociación tan maravillosa como Acción Social por la Música. Gracias a nuestro corto pudimos conseguir una donación de 20.000 euros para la asociación.

Licencias y certificaciones



Digital Photography
Alison - Free Online Learning
ID de la credencial: 591-8581164
Ver credencial



Nivel B2 en inglés
Centro Superior de Idiomas Modernos, UCM

Idiomas

Español
Competencia bilingüe o nativa

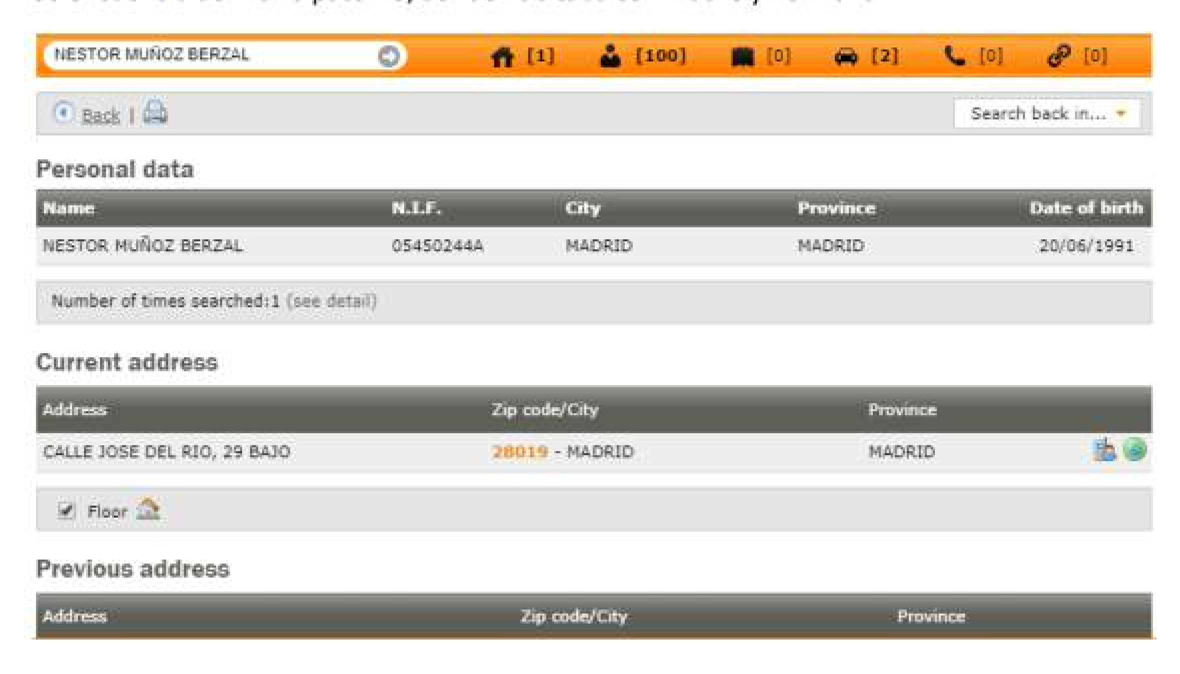
Inglés
Competencia básica profesional

En resumen estamos ante alguien con conocimientos de seguridad informática, anonimato en la red, administración de servidores y experiencia en comunicaciones.

Ahora tenemos un plus de información sobre nuestro objetivo: (https://www.inglobaly.com/)

Se realiza búsqueda en base de datos de empresa por nombre y apellidos y por DNI sin resultado positivo.

Se encuentra domicilio paterno, donde habitaba con madre y hermana:



NESTOR MUÑOZ BERZAL [1] [100] [0] [2] [0] [0]

Back | Search back in...

Personal data

Name	N.I.F.	City	Province	Date of birth
NESTOR MUÑOZ BERZAL	05450244A	MADRID	MADRID	20/06/1991

Number of times searched:1 (see detail)

Current address

Address	Zip code/City	Province
CALLE JOSE DEL RIO, 29 BAJO	28019 - MADRID	MADRID

Floor

Previous address

Address	Zip code/City	Province



Results of the Research

Address	CALLE JOSE DEL RIO 29, piso BAJO (28019)	
	Surname, Name	Year of birth:
	BERZAL BARROSO, MARIA LUISA	1965
	MUÑOZ BERZAL, NESTOR	1991
	MUÑOZ BERZAL, BARBARA	1994

Found 1 records

Se localiza una multa de tráfico de 2013 en el siguiente documento

https://s3-eu-west-1.amazonaws.com/testra.paginas/83be2f1cc2d9bd4542fca4bb8dea6ce5?Signature=70%2B6YnHwEzZAaDS%2By%2BgRuqWG1ic%3D&AWSAccessKeyId=AKIAJTAU2GNN2JY66H2Q&Expires=1584960904



280135641470	MUÑOZ BERZAL, NESTOR	05450244A	MADRID	01/03/2013	M7937PU

El vehículo sancionado es un Ford fiesta 1.1 del año 1994

Finalizo la primera parte de mi post con estas ideas importantes:

* Que gracias a los headers pudimos identificar que las huellas dígitales de los sitios lulzwrzcle5ks3se.onion, bcloud2suoza3ybr.onion, society44nlbxqdz.onion y kowloon5aibdbege.onion son idénticas, además que el resultado de mi experimento de denegación de servicio hacia un sólo dominio (el del cebolla chan) tiró todos los sitios mencionados al principio significa que todos están alojados en el mismo servidor que vendría a ser el hosting de Kowloon Hosting Services, el cual no actualiza su home page desde 2018, mismo año en que cebolla chan volvió a estar en línea.

* Dado el caso que el moderador nestor dejó abandonada su cuenta de forma prematura, siendo el usuario #5 creado (El #4 no existe, lo que significa que fué borrado) puede significar varias cosas:

- El usuario abandonó el proyecto.

- La cuenta de usuario es tan sólo una cuenta alternativa del administrador para simular actividad.

El usuario nestor ha demostrado tener amplio conocimiento en la materia, al igual que Sysop, al recomendar hacer uso de sitios sin javascript, creando sitios como blackcloud o society, recomendando el uso de cifrado y whonix, podría arriesgarme a decir que ambos son la misma entidad o están muy relacionados.

* Que utilizando recursos disponibles libremente en internet se trazó una correlación de su identidad en la red tor, hasta su identidad en el mundo real de la siguiente forma:

Perfil Nestor → Nes Web → hackerlabs.es → Nombre real “Nestor” → Uso de nick Nes en patente.

* Que es curioso el hecho que estuviera activo en retormar hackerlabs en abril de 2018 al mismo tiempo que el foro cebolla chan se volvía a poner en marcha.

* Que partiendo desde tan sólo una correlación pudimos dar con mucha info personal de un objetivo, eso demuestra que tan importante es cuidar nuestro opsec en internet y que sin importar las tecnologías que usemos, si no las sabemos aplicar, serán tan sólo una puerta sin llave.